

Windows and Office Deployment Lab Kit

Windows 10 Enterprise | Microsoft 365 Apps for enterprise | Enterprise Mobility + Security

Lab Guide

Updated: November 16, 2021

**Table of Contents**

[1 Introduction 3](#_Toc75417699)

[2 Lab Set Up 5](#_Toc75417700)

[2.1 On-Premises Environment 5](#_Toc75417701)

[2.2 Cloud Environment 7](#_Toc75417702)

[2.3 On-Premises Environment Setup 12](#_Toc75417703)

[2.4 Cloud Environment Set Up 26](#_Toc75417704)

[3 Plan and Prepare Infrastructure 33](#_Toc75417705)

[3.1 Desktop Analytics 33](#_Toc75417706)

[3.2 Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP) 39](#_Toc75417707)

[3.3 Tenant Attach, Co-Management and Switching Workloads 52](#_Toc75417708)

[3.4 Endpoint Analytics 58](#_Toc75417709)

[3.5 Remote Access (VPN) 59](#_Toc75417710)

[4 Prepare Configuration 71](#_Toc75417711)

[4.1 Optimize Windows 10 Update Delivery 71](#_Toc75417712)

[4.2 Servicing Windows 10 using Group Policy 73](#_Toc75417713)

[4.3 Servicing Windows 10 using Microsoft Intune 74](#_Toc75417714)

[4.4 Servicing Windows 10 with Configuration Manager 84](#_Toc75417715)

[4.5 Servicing Microsoft 365 Apps for enterprise using Configuration Manager 88](#_Toc75417716)

[4.6 Servicing Microsoft 365 Apps for enterprise using Intune 97](#_Toc75417717)

[4.7 Security and Compliance 97](#_Toc75417718)

[5 Prepare Applications 145](#_Toc75417719)

[5.1 Readiness Toolkit for Office 145](#_Toc75417720)

[5.2 MSIX Packaging and Conversion of Win32 Applications 146](#_Toc75417721)

[6 Deploy Windows 10 150](#_Toc75417722)

[6.1 OS Deployment Task Sequences in Configuration Manager 150](#_Toc75417723)

[6.2 OS Deployment Task Sequences in MDT 165](#_Toc75417724)

[6.3 Windows AutoPilot 167](#_Toc75417725)

[6.4 Deploy and manage the new Microsoft Edge 183](#_Toc75417726)

[7 Deploy Microsoft 365 Apps for enterprise 198](#_Toc75417727)

[7.1 Cloud Managed Deployment 198](#_Toc75417728)

[7.2 Locally Managed Deployment 201](#_Toc75417729)

[7.3 Microsoft 365 Apps for enterprise Deployment on Non-AD Joined Devices 205](#_Toc75417730)

[7.4 Enterprise Managed Deployment using Configuration Manager 211](#_Toc75417731)

[7.5 Enterprise Managed Deployment using Microsoft Intune 218](#_Toc75417732)

[7.6 LOB Deployment and Management with Microsoft Intune 219](#_Toc75417733)

[7.7 Deploy Microsoft Teams 221](#_Toc75417734)

[7.8 Assignment Filters 224](#_Toc75417735)

[8 Appendix A: Windows Virtual Desktop 227](#_Toc75417736)

[8.1 Windows Virtual Desktop – Prepare 227](#_Toc75417737)

[8.2 Windows Virtual Desktop – Deploy 229](#_Toc75417738)

[8.3 Windows Virtual Desktop – Optimize 234](#_Toc75417739)

[9 Appendix B - Compatibility 238](#_Toc75417740)

[9.1 Convert a Win32 app to a UWP app 238](#_Toc75417741)

[9.2 Windows App Certification Kit 245](#_Toc75417742)

[10 Appendix C - User File and Settings Migration 248](#_Toc75417743)

[10.1 Known Folder File Migration 248](#_Toc75417744)

[10.2 User State Migration Tool 256](#_Toc75417745)

[10.3 Enterprise State Roaming 263](#_Toc75417746)

[10.4 Start Menu Customization and UWP App Removal 264](#_Toc75417747)

[10.5 User Experience Virtualization (UE-V) 266](#_Toc75417748)

[10.6 Application Self-Service with Microsoft Store for Business 267](#_Toc75417749)

[11 Appendix D: Prepare infrastructure 270](#_Toc75417750)

[11.1 Outlook Mailbox Hosted Cache Reduction via Group Policy 270](#_Toc75417751)

[11.2 CMPivot for real-time data in Configuration Manager 272](#_Toc75417752)

[11.3 Outlook Mobile App Config and App Protection 272](#_Toc75417753)

# Introduction

The labs in this guide are designed to help you plan, test, and validate your deployment and management of desktops running Windows 10 Enterprise and Microsoft 365 Apps for enterprise. The labs cover using Microsoft Endpoint Configuration Manager, Desktop Analytics, Office Customization Tool, OneDrive, Windows Autopilot and more.

This kit is highly recommended for organizations preparing for Windows 8 upgrades, and also applies if you're currently using Windows 10, Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus), or Office 2019. Additionally, as an isolated environment, the lab is ideal for exploring deployment tool updates and testing your deployment-related automation. The guide is divided into five sections:

**Note:** This lab guide is not intended to cover all deployment and management tasks and scenarios. For comprehensive guidance, including scenarios that can be tested directly in the lab environment accompanying this lab guide, see: [Microsoft 365 documentation](https://docs.microsoft.com/en-us/microsoft-365/?view=o365-worldwide).

1. **Lab Set Up:** This section guides you through the steps required for setting up the on-premises lab environment and joining it to trial versions of Azure and Intune. This will provide you with the full Microsoft 365 infrastructure required to work through all scenarios in the lab.
2. **Plan and prepare infrastructure.** For a successful deployment you must first know what you have. That means taking an inventory of your devices and apps and verifying compatibility. Desktop Analytics can help with this, allowing you tap into compatibility intelligence and diagnostic data gathered from hundreds of millions of PCs. Additionally, this section details how to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune. Co-management can help you get more out of your existing Configuration Manager deployment by unlocking additional cloud-powered capabilities like conditional access.
3. **Prepare configuration.** This chapter focusing on servicing your infrastructure. This represents a major shift in the way you maintain users’ desktop real-estate, providing new capabilities, experiences, and protections to your user. Additionally, we focus on security. It is important you familiarize yourself with the new built-in capabilities in both Windows and Office and compare those with what you already have.
4. **Prepare applications.** This section covers two tools to help new and legacy applications for installation: 1. The Readiness Toolkit for Office add-ins and VBA can help you identify compatibility issues with your Microsoft Visual Basic for Applications (VBA) macros and add-ins that you use with Office. 2. The MSIX Packaging Tool enables you to repackage your existing desktop applications to the MSIX format
5. **Deploy Windows 10.** With everything prepared, the next step is to deploy the OS images. A lot of the heavy lifting can be done using Configuration Manager task sequences and infrastructure. This section also covers deployment and management of the new Microsoft Edge.
6. **Prepare/Deploy Microsoft 365 Apps for enterprise.** In these sections, we show you how to prepare your apps for automated deployments, and that you are set up for success whether your apps deploy using Click-to-Run, MSIX, or conventional MSI-based.

Additionally, this guide includes an Appendix which covers other scenarios that may be applicable to your deployment planning, including app compatibility scenarios, User File and Settings Migration, Windows Virtual Desktop and more.

# Lab Set Up

It is important that this section be completed after following the steps in the **Lab Set Up Guide** and before proceeding with the lab activities. The following requirements for each environment (on-premises and cloud) to support the labs.

Note: When you are going through the Labs, you might notice that there is repetition of certain steps and conflicts. Therefore, it is recommended that once you are done with a specific lab, reverse the changes made to avoid those conflicts from the VMs and Physical Machines as well as Azure, Intune and Microsoft 365.

## On-Premises Environment



### Prerequisites

Listed below are the requirements for the on-premises environment:

|  |  |
| --- | --- |
| Complete | Task |
|  | The customer will provide a total of five (5) **client** devices.   * Three (3) devices that have a new or corporate image–based installation of Windows 7 Release to Manufacturing (RTM) or later, running a sample of customer applications. If possible, include at least one touch device. These devices will be used for the labs on Windows 10 in-place upgrade and BIOS to UEFI conversion. * Two (2) devices of the same architecture (32-bit or 64-bit) that can be formatted or do not have a corporate image installed that are compatible with Windows 10 hardware specifications. These devices will be used for the labs on Wipe and Load and Credential Guard. |
|  | One (1) **physical** server or workstation to host the virtual lab environment. The requirements are listed below:   * **Operating System**: Windows Server 2016, 2012 R2, or Windows 10 with Hyper-V installed (recommended to use Windows Server OS) and fully updated. Administrative rights on the host. * **Memory**: Up to 32 GB. * **Disk Space**: At least 300 GB or more. * **Disk Subsystem**: High throughput/speed. * **Ethernet**: Two (2) or more Gb NICs. * **Network Connections**: Internet connection and lab switch. * **Applications**: Microsoft Azure PowerShell modules installed (<https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-3.8.0>). |
|  | One (1) gigabit network lab **switch** with sufficient ports to connect client devices and lab environment. |
|  | Download the Windows 10 Enterprise dev environment for Hyper-V. <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines> |
|  | Download the latest Windows 10 from MSDN or VLSC that matches the architecture of the current image installed on the client devices. |
|  | Download the latest Windows 10 Assessment and Deployment Kit. <https://go.microsoft.com/fwlink/?linkid=2120254> |
|  | *[OPTIONAL]* Provide the source of any security guidance that is being used with HTML Reports and GPO Backups. |

### Configuration

The on-premises environment is configured by using the Windows and Office Deployment Lab Kit, which can be accessed in the [Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-365-modern-desktop-lab-kit) here. Follow the Windows and Office **Lab Kit Setup Guide** to provision the virtual machines on Hyper-V.

When setup is complete, the following virtual machines are configured and the deployment lab system is available for use.

| Server Name | Roles & Products |
| --- | --- |
| HYD-APP1 | Microsoft BitLocker Administration and Monitoring  Microsoft SQL Server 2017 |
| HYD-CLIENT1 | Windows 10 21H1 Domain Joined |
| HYD-CLIENT2 | Windows 10 21H1 Domain Joined |
| HYD-CLIENT3 | Windows 10 21H1 Workgroup |
| HYD-CLIENT4 | Windows 10 21H1 Workgroup |
| HYD-CLIENT 5, 6 | Bare metal (No Installations) |
| HYD-CLIENT7 | Windows 7 SP1 Domain Joined |
| HYD-CM1 | Microsoft Endpoint Configuration Manager 2103  Windows Deployment Services  Microsoft Deployment Toolkit  Windows Assessment and Deployment Kit for Windows 10, version 2004  Windows Software Update Services  Microsoft SQL Server 2017 |
| HYD-DC1 | Active Directory Domain Controller, DNS, DHCP, Certificate Services |
| HYD-GW1 | Remote Access for Internet Connectivity |
| HYD-INET1 | Simulated Internet |
| HYD-MDT1 | Microsoft Deployment Toolkit  Windows Assessment and Deployment Kit for Windows 10, version 2004  Windows Deployment Services |
| HYD-VPN1 | Remote Access for VPN |

The table below lists the credentials and access type available in the default implementation:

| User | Access Type | User Name | Password |
| --- | --- | --- | --- |
| Local Administrator | Administrative | Administrator | P@ssw0rd |
| Domain Administrator | Enterprise Administrator | CORP\LabAdmin | P@ssw0rd |

## Cloud Environment

Certain lab scenarios require the cloud environment. Follow the steps below to configure and prepare the required cloud services.

Listed below are the requirements for the cloud environment used for various labs in this guide.

|  |  |
| --- | --- |
| Complete | Task |
|  | Provide licensed **subscriptions** or sign-up for a trial subscription for the following Microsoft Cloud Services.   * **Microsoft Azure**: <https://azure.microsoft.com/en-us/free/> * **Enterprise Mobility + Security:** <http://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-trial> (configured as part of the Lab Setup) * **Windows Defender Advanced Threat Protection:** <http://www.microsoft.com/en-us/WindowsForBusiness/windows-atp> (configured as part of the Lab Setup) * **Microsoft 365 E3:** Configured as part of the Lab Setup.   **Note**: All trial tenants have an evaluation period. These subscriptions/tenants will expire unless they are extended or if the customer purchases the system.  **Note**: It is possible to use an existing trial subscription if the engagement dates are within the evaluation period.  **Note**: An appropriate MSDN subscription could be used to activate the Azure Benefit for 30 days. |

### Set up Azure and Microsoft 365

In this section, you will create an Azure AD and a Microsoft 365 Trial Tenant used for the later lab environment.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Azure AD | **Note:** If Azure AD is already present and associated with a Subscription, then skip this section.   1. Open an InPrivate Browser session. 2. Navigate to <https://portal.azure.com> 3. Sign in with the **email address** associated with your Azure subscription. 4. On the left navigation bar, click **Create a resource > Identity > Azure Active Directory**. 5. In the Create directory pane fill in the following values:   ORGANIZATION NAME: **<CompanyName>**  INITIAL DOMAIN NAME: **<AzureDomainName>**  COUNTRY OR REGION: **Choose a region**   1. Click **Create**.   **Note**: This may take a couple of minutes to complete. |
| Create Azure AD Admin User | 1. Sign out from Azure portal and sign back in again. 2. Click your **email address** on the upper right corner and click **Switch directory**. Select **<AzureDomainName>.onmicrosoft.com**. If required, refresh the page for the directory to be visible. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Users** and then click **+ New user**. 5. In the New user pane, fill in the following values:   USER NAME: **<LabAdmin>** (Suggestion: LabAdmin@<AzureDomainName>.onmicrosoft.com)  NAME: **<Admin Name>**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name   1. Select **Auto-generate password** and select **Show Password** and write down the temporary password **<OldLabAdminPassword>**. 2. Click on **User** next to **Roles**, select **Global administrator** and **Desktop Analytics administrator**, then click **Select**.   **Note:** The Desktop Analytics administrator role is required here for the Desktop Analytics scenario only.   1. Click **Create**. |
| Resetting the Password | 1. Logout from Azure Portal. 2. Log in to Azure Portal using **LabAdmin** account. 3. Type in the **<OldLabAdminPassword>** that you wrote down. 4. Type the new password: **<NewLabAdminPassword>**. 5. Confirm the new password and sign in. |
| Associate a Subscription with the New Azure AD Tenant | **Note**: If Azure AD is already present and associated with a Subscription, then skip this section.   1. Click **All services > Subscriptions**. 2. Click **Add** to add a new subscription to the new Azure AD Tenant. 3. If you are eligible for a Free Trial, then click **Free Trial** or select any other offer from the list. 4. Follow the instructions for **Azure – Sign up**. 5. At the end you must be able to see a valid Active Subscription with a Subscription ID in the **All services > Subscriptions** pane. |
| Subscribe to Microsoft 365 E3 Trial Subscription | 1. Open a new tab and navigate to <https://portal.office.com>. 2. Click the **Admin** tile. 3. Click **Billing | Purchase services**. 4. Search for and select **Microsoft 365 E3** and then click **Get free trial**. 5. Follow the usual procedure for verification and click **Try now | Continue**. You should now be able to see the subscription under **Billing | Your products**. |
| Create Azure Test Users | 1. Navigate to <https://portal.azure.com>. 2. Sign in with the email address associated with your Azure subscription if required. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Users** and then click **+ New user**. 5. In the New user pane, fill in the following values:   USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**  NAME: **Test User1**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name   1. Select **Auto-generate password** and select **Show Password** and write down the temporary password. 2. Click **Create**. 3. Repeat **Steps 30 – 36** for a second user as follows:   USER NAME: **TU2@<AzureDomainName>.onmicrosoft.com**  NAME: **Test User2**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name |
| Set Password for your New Users using Microsoft 365 | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://login.microsoftonline.com>. 4. Log in with the user account created **TU1@<AzureDomainName>.onmicrosoft.com** 5. Type in the **temporary password** that you wrote down. 6. Type the New Password: **<newuserpassword>** 7. Confirm the new Password: **<newuserpassword>** 8. Click **Sign in**. 9. Repeat **Steps 38-45** for **TU2@<AzureDomainName>.onmicrosoft.com** 10. Close all browser windows. |
| Create Azure AD Group (Sales) | 1. Open an InPrivate Browser session. 2. Navigate to <https://portal.azure.com> 3. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 5. Click **+ New group**. 6. In the New Group pane fill in the following values:   Group type: **Microsoft 365**  Group name: **Sales**  Membership type: **Assigned**  Members: **Test User1** and **Test User2**   1. Click **Create**. |

### Set up Enterprise Mobility + Security

In this section, you will create an Intune Trial Tenant that will be used later on in the lab. This tenant will be created using the Azure AD that you created in the previous lab.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Sign Up for a Trial Microsoft Intune Subscription | 1. Start a new Internet Explorer window in private mode. 2. Navigate to <https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-trial> and click **Free trial** and then click **Sign in**. 3. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. Click **Try now** to confirm your order. 5. Click **Continue**. 6. On the left navigation bar, click **Billing > Your products** and verify that the **Enterprise Mobility + Security E5 Trial** is **Active**. |

### Enable and Configure Cloud Services

In the section, you will assign licenses and configure additional cloud services that will be used in the lab environment.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Assign Microsoft 365 E3 and EM+S Licenses | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.office.com> and **Sign in** with **labadmin@<AzureDomainName>.onmicrosoft.com**. Click the **Admin** tile. 4. On the left navigation bar, click **Users > Active users**. 5. Select all **LabAdmin**, **Test User1** and **Test User2** then click the **Manage product licenses** action by clicking the (**…**). Select **Add to existing product license assignments** and click **Next**. 6. Select the appropriate **Location**, enable **Microsoft 365 E3** and **Enterprise Mobility + Security E5**. 7. Ensure all the checkboxes are selected. Ignore the checkboxes which are greyed out or cannot be selected. 8. Click **Add** and then click **Close**. **Note:** Ensure that all the 3 users have all the product licenses assigned. |
| Enable Device Registration | 1. Close all browser windows. 2. Open an **InPrivate Browser** session. 3. Navigate to <https://portal.azure.com>. 4. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 5. On the left navigation bar, click **Azure Active Directory > Devices > Device settings**. 6. In the **Users may join devices to Azure AD** setting, select **All** if not selected. 7. In the **Users may register their devices with Azure AD** setting, select **All**. 8. Click **Save**. |
| Enable Windows Defender ATP Trial | **Note**: A trial application should have been started before proceeding with the steps - <https://www.microsoft.com/en-us/windowsforbusiness/windows-atp>   1. Close all browser windows. 2. Open an InPrivate Browser session. 3. Navigate to <https://www.microsoft.com/en-us/windowsforbusiness/windows-atp> and click **Start free trial**. 4. Check the box next to **I accept these terms and conditions** and click **Next**. 5. On the Please enter your details below page, enter your details and click **Submit**. 6. You will get a message stating that the Windows Defender Advanced Threat Protection Team will review your application and contact you via email within 7 business days. Once your application is approved, you will then receive an invitation email with onboarding instructions. 7. Within 7 business days, you will then receive an email to activate your trial and all the onboarding instructions. Click **Activate your trial now**. Download the **setup guide**. The setup guide also contains instructions and links for the attack demo. 8. During activation, click **Sign in**. 9. **Sign in** with **LabAdmin@<AzureDomainName>.onmicrosoft.com** 10. Click **Try now**. 11. Click **Continue**. 12. Close all browser windows. |

## On-Premises Environment Setup

Perform once the on-premises environment provisioning is complete.

### Servicing Configuration Manager

Configuration Manager uses an in-console service method called Updates and Servicing that makes it easy to locate and then install recommended updates for your Configuration Manager infrastructure. This in-console servicing method is supplemented by out-of-band updates such as hotfixes that are intended for customers who need to resolve issues that might be specific to their environment. These in-console updates replace on-premises update delivery methods.

In this section, you will learn how to use the Configuration Manager console to locate and install updates that provide fixes and new capabilities to your Configuration Manager infrastructure and clients.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

### Configure as Online Mode

In this activity, you will locate and install Configuration Manager updates from the internet-connected site server. Follow this activity if your environment **has an internet connection** (if not, move to the next activity).

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Enable Service Connection Point (if already not installed) | 1. Open the **Configuration Manager Console** from the Start Menu. 2. In the Warning dialog box, click **OK** if it appears. 3. Browse to **Administration > Site Configuration >** **Servers and Site System Roles**. 4. Right-click on **\\CM1.corp.contoso.com** and select **Add Site System Roles**. 5. In the **General** page, click **Next**. 6. In the **Proxy** page, click **Next**. 7. In the **System Role Selection** page, select **Service connection point** and click **Next**. 8. In the **Service Connection Mode** page, select **Online, persistent connection (recommended)** then click **Next**. 9. In the **Summary** page, click **Next**. 10. In the **Completion** page, click **Close**. |
| Install New Updates (if available) | **Note**: Perform the succeeding steps if there is a newer Configuration Manager build available after 2010. Otherwise, proceed to **3.3.2**.  **Note**: If the update installation is suspended at “**Downloading**” state for extended period of time, restart the **SMS\_EXECUTIVE** (smsexec) service.   1. In the **Configuration Manager Console**, browse to **Administration > Updates and Servicing**.   **Note:** It will first download the update before it is made Available. If already not downloaded, then select **Configuration Manager 200x** and then click **Download**. Click **OK**.   1. In the **Updates and Servicing** pane, select an **Available** update (**Configuration Manager 200x**) and then click **Install Update Pack**. 2. In the **General** page, select **Ignore any prerequisite check warnings and install this update regardless of missing requirements** and click **Next**. 3. In the **Features** page, select **all** available features then click **Next**. 4. In the **Client Update Options** page, click **Next**. 5. In the **License Terms** page, select **I accept these License Terms** **and Privacy Statement** and click **Next**. 6. In the **Summary** page, click **Next**. 7. In the **Completion** page, click **Close**.   **Note**: The 200x upgrade installation may take up to an hour. |
| Upgrade the Configuration Manager Console and Validate Version Number | 1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. In the Warning window, click **OK** to upgrade the Configuration Manager Console.   **Note:** At this stage, the Configuration Manager Console will close. The update will be downloaded and installed and the Configuration Manager Console will be reopened. Click **OK** if there are any hotfixes pertaining to (**Configuration Manager 200x**) available.   1. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 200x**) is Installed.   **Note:** Install any available hotfixes pertaining to (**Configuration Manager 200x**).   1. After the upgrade, in the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 200x). 4. Reboot **CM1** once. |

### Configure as Offline Mode *(OPTIONAL)*

In the activity, you will locate and install Configuration Manager updates from another computer that has internet connection. Follow this section if your environment has **no internet connection**.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Enable Service Connection Point (if already not installed) | 1. Open the **Configuration Manager Console** from the Start Menu. 2. In the Warning dialog box, click **OK** if it appears. 3. Browse to **Administration > Site Configuration >** **Servers and Site System Roles**. 4. Right-click on **\\CM1.corp.contoso.com** and select **Add Site System Roles**. 5. In the **General** page, click **Next**. 6. In the **Proxy** page, click **Next**. 7. In the **System Role Selection** page, select **Service connection point** and click **Next**. 8. In the **Service Connection Mode** page, select **Offline, on-demand connection** then click **Next**. 9. In the **Summary** page, click **Next**. 10. In the **Completion** page, click **Close**. |
| Prepare Usage Data | 1. Download and extract the EXE from <https://www.microsoft.com/en-in/evalcenter/evaluate-system-center-configuration-manager-and-endpoint-protection> and copy the folder **ServiceConnectionTool** from **SMSSETUP\Tools** to **C:\**. 2. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 3. **Execute** the following command:   **serviceconnectiontool.exe -prepare -usagedatadest .\UsageData.cab** |
| Upload Usage Data and Download Updates from an Internet-connected Remote Computer | 1. **Copy** the folder **C:\ServiceConnectionTool** from **CM1** to the root drive of the computer that has **internet connection**. 2. From the computer that has internet connection, open an **Administrative Command Prompt** and browse to the copied **ServiceConnectionTool** folder. 3. **Execute** the following command:   **md .\UpdatePacks**   1. **Execute** the following command:   **Serviceconnectiontool.exe -connect -usagedatasrc .\UsageData.cab updatepackdest .\UpdatePacks** |
| Import Updates | 1. From the computer that has **internet connection**, copy the **UpdatePacks** folder to **CM1** in the folder **C:\ServiceConnectionTool**. 2. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 3. **Execute** the following command:   **serviceconnectiontool.exe -import -updatepacksrc .\UpdatePacks** |
| Force Refresh | 1. In the **Configuration Manager Console**, browse to **Monitoring > System Status >** **Component Status**. 2. In the ribbon, select **Start >** **Configuration Manager Service Manager**. 3. In the **Configuration Manager Service Manager** window, expand **CHQ > Components >** **SMS\_EXECUTIVE**. 4. On the right pane, **right-click** on **SMS\_EXECUTIVE** and select **Stop**. 5. Right-click on **SMS\_EXECUTIVE** and select **Query**. 6. Once the **Status** of SMS\_EXECUTIVE changes to **Stopped**, **right-click** **SMS\_EXECUTIVE** and select **Start**. |
| Install New Updates (if available) | **Note**: Perform the succeeding steps if there is a newer Configuration Manager build available after 2002. Otherwise, proceed to section **3.3.2**.   1. In the **Configuration Manager Console**, browse to **Administration > Updates and Servicing**. 2. In the **Updates and Servicing** pane, select the **Configuration Manager 200x** update and then click **Install Update Pack**. 3. In the **General** page, click **Next**. 4. In the **Features** page, select **all** available features then click **Next**. 5. In the **Client Update Options** page, click **Next**. 6. In the **License Terms** page, select **I accept these License Terms** **and Privacy Statement** and click **Next**. 7. In the **Summary** page, click **Next**. 8. In the **Completion** page, click **Close**.   **Note**: The 200x upgrade installation may take up to an hour. |
| Upgrade the Configuration Manager Console and Validate Version Number | 1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. In the Warning window, click **OK** to upgrade the Configuration Manager Console.   **Note:** At this stage, the Configuration Manager Console will close. The update will be downloaded and installed and the Configuration Manager Console will be reopened. Click **OK** if there are any hotfixes pertaining to (**Configuration Manager 200x**) available.   1. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 200x**) is Installed.   **Note:** Install any available hotfixes pertaining to (**Configuration Manager 200x**).   1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 200x). 4. Reboot **CM1** once. |

### Prepare Configuration Manager (if not already configured)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure and Validate Discovery Methods | 1. Open the **Configuration Manager Console** from the Start Menu. 2. Navigate to **Administration > Hierarchy Configuration >** **Discovery Methods**. 3. Right-click **Active Directory Forest Discovery** and click **Properties**. 4. Check the box next to **Automatically create Active Directory site boundaries when they are discovered** and uncheck the box next to **Automatically create IP address range boundaries for IP subnets when they are discovered**. 5. Click **Apply** and then click **OK**. 6. Click on **Active Directory Forest Discovery** and select **Run Forest Discovery Now** from the ribbon bar. 7. Click **Yes** on the dialog box. 8. Right-click **Active Directory Group Discovery** and click **Properties**. 9. Double-click the discovery scope already present. 10. Select the option **Specify an account** and click **Set… >** **New Account**. 11. Enter the User name: **CORP\LabAdmin**, Password: **P@ssw0rd** and Confirm password: **P@ssw0rd**, click **Verify** and test the connection to the Active Directory Data source Path: **LDAP://DC=corp,DC=contoso,DC=com**, click **OK** on the prompt once successful. Click **OK**. Click **OK** again. 12. Click the **Options** tab and select the checkboxes next to **Only discover computers that have logged on to a domain in a given period of time**, **Only discover computers that have updated their computer account password in a given period of time** and **Discover the membership of distribution groups**. 13. Click **Apply** and then click **OK**. 14. Click on **Active Directory Group Discovery** and select **Run Full Discovery Now** from the ribbon bar. 15. Click **Yes** on the dialog box. 16. Right-click **Active Directory System Discovery** and click **Properties**. 17. Double-click the active directory container already present. 18. Check the box next to **Discover objects within Active Directory groups**. 19. Select the option **Specify an account**, click **Set**… > **Existing Account**. 20. In the **Select Account** window, select **corp\labadmin** then click **OK** twice. 21. Click **Apply** and then click **OK**. 22. Click on **Active Directory System Discovery** and select **Run Full Discovery Now** from the ribbon bar. 23. Click **Yes** on the dialog box. 24. Right-click **Active Directory User Discovery** and click **Properties**. 25. Double-click the active directory container already present. 26. Check the box next to **Discover objects within Active Directory groups**. 27. Select the option **Specify an account**, click **Set**… > **Existing Account**. 28. In the **Select Account** window, select **corp\labadmin** then click **OK** twice. 29. Click **Apply** and then click **OK**. 30. Click on **Active Directory User Discovery** and select **Run Full Discovery Now** from the ribbon bar. 31. Click **Yes** on the dialog box. 32. Ensure that **Heartbeat Discovery** is already **Enabled**. |
| Configure and Validate Boundaries | 1. Navigate to **Administration > Hierarchy Configuration >** **Boundaries**. 2. Ensure that the **Default-First-Site-Name** boundary is already created. 3. Navigate to **Administration > Hierarchy Configuration >** **Boundary Groups**. 4. Ensure that the **Corp Boundary Group** is already created. |
| Configure an IP Based Boundary | 1. First, in **DC1**, click **Start > Windows Administrative Tools > Active Directory Sites and Services**. 2. Expand **Sites**, right-click **Subnets** and then click **New Subnet**. 3. In the **Prefix** field, enter **10.0.0.0/24**, select **Default-First-Site-Name** and then click **OK**. 4. Back in **CM1**, navigate to **Administration > Hierarchy Configuration >** **Boundaries**. 5. Right-click **Boundaries** and click **Create Boundary**. 6. In the **Description** field enter **IP Based Boundary**, for **Type** select **IP subnet**, in the **Network** field enter **10.0.0.0** and in the **Subnet mask** field enter **255.255.255.0**. 7. Click the **Boundary Groups** tab and click **Add**. 8. Select **Corp Boundary Group** and click **OK**. 9. Click **Apply** and click **OK**. |
| Configure Boundary Group and DP Group for the DP | 1. Navigate to **Administration | Distribution Points**. 2. Right-click the distribution point and click **Properties**. 3. Click the **Group Relationships** tab and click **Add**. 4. Select **Corp DPs** and click **OK**. 5. Click the **Boundary Groups** tab. 6. Click **Add**. 7. Select **Corp Boundary Group** and click **OK**. 8. Click **Apply** and click **OK**. |
| Configure and Validate the Network Access Account | 1. Navigate to **Administration > Site Configuration >** **Sites**, select the site and click **Settings > Configure Site Components >** **Software Distribution**. 2. Click the **Network Access Account** tab. You will see a network access account already in the list. Select and click the **cross** button to delete it. 3. Click **Yes** on the prompt. 4. Click the **star** and click **New Account**. 5. Enter the User name: **CORP\LabAdmin**; Password and Confirm password: **P@ssw0rd**; click **Verify** and in the Network share: enter **\\cm1\SMS\_CHQ**; click **Test connection** and click **OK** once successful. Click **OK** again. 6. Click **Apply** and then click **OK**. |
| Configure and Validate the Client Push Installation | 1. Navigate to **Administration > Site Configuration >** **Sites**. 2. Right-click on the **CHQ** site then select **Client Installation Settings >** **Client Push Installation**. 3. In the **General** tab, select **Enable automatic site-wide client push installation** and **Allow connection fallback to NTLM**. Ensure that **Servers** and **Workstations** are checked and **Never install the Configuration Manager client on domain controllers unless specified in the Client Push Installation Wizard** is selected. 4. In the **Accounts** tab, Click the **star** button and click **Existing Account**. 5. In the **Select Account** window, select **corp\labadmin** then click **OK.** 6. Review the **Installation Properties** tab. Click **Apply** and then click **OK**. |

### 

### Create Test VMs

#### Download MSDN & EVAL ISOs

These ISOs will be used to create VMs that will be used in various chapters within the lab.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the HYPER-V Host.** | |
| Download Windows 7 ISO (MSDN) | 1. Open Internet Explorer and browse to the URL below.   <https://msdn.microsoft.com/subscriptions/securedownloads/>   1. From the website, Sign-in with your MSDN registered account. 2. On the **Search** field, enter **Windows 7 Enterprise with Service Pack 1**. 3. **Search** for **Windows 7 Enterprise with Service Pack 1 (x64) – DVD (English)** and **Download** to C:\. |
| Download Windows 10 20H2 ISO (MSDN) | 1. Open Internet Explorer and browse to the URL below.   <https://msdn.microsoft.com/subscriptions/securedownloads/>   1. From the website, Sign-in with your MSDN registered account. 2. On the **Search** field, enter **Windows 10**. 3. **Search** for **Windows 10 (business editions), Version 20H2 (x64) – DVD (English)** and **Download** to C:\ |
| Download Windows 10  ISO (EVAL) | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-in/evalcenter/evaluate-windows-10-enterprise>   1. Select **ISO – Enterprise** ***(latest version)*** and click **Continue**. 2. Fill in all the fields to complete the form and click **Continue** again. 3. Select **64 bit**, select your language and click **Download**. |

#### Build a Windows 7 Client Machine

For this task, you will build, and domain-join a Windows 7 virtual machine that will be used to perform the upgrade later.

**Note:** The **WIN7** VM, will be used for the following scenarios in this Lab Guide:

* Section 6.1.2 - PC Refresh
* Section 6.1.3 - PC Replacement
* Section 6.1.4.2 - Perform an In-Place Upgrade of Windows 7 Using Configuration Manager (Current Branch)
* Section 6.3.8 - AutoPilot for Existing Devices
* Section 10.2.1 – USMT - PC Refresh
* Section 10.2.1 – USMT - PC Replacement

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the HYPER-V Host and the New Generation 1 virtual machine.** | |
| Create the Virtual Machine | * + - 1. On the Hyper-V Host server, launch **Hyper-V Manager**.       2. Under **Actions**, click **New > Virtual Machine**.       3. On the **Before You Begin** page, click **Next**.       4. On the **Specify Name and Location** page, provide a Name (e.g. **WIN7**). Based on where you want to store virtual machine files, click **Store the virtual machine in a different location** and **Browse** to that specific location. Click **Next**.       5. On the **Specify Generation** page, select **Generation 1** and click **Next**.       6. On the **Assign Memory** page, provide a Startup memory of **2048 MB** or more and click **Next**.       7. On the **Configure Networking** page, in the Connection drop-down, select **HYD-CorpNet** and click **Next**.       8. On the **Connect Virtual Hard Disk** page, keep the defaults and click **Next**.       9. On the **Installation Options** page, select **Install an operating system from a bootable CD/DVD-ROM** and **Browse** to the ISO image as stated in **Section 2.3.5.1**. Click **Next**.       10. On the **Summary** page, review and click **Finish**.       11. Click **Start** to turn on the VM and proceed with the installation. Join the system to the **corp.contoso.com** domain using the domain administrator credentials (**corp\labadmin**).       12. Log in as **CORP\LabAdmin** and then turn off the **Windows Firewall Mode** for **Domain network location settings, Home or work (private) network location settings and Public network location settings**. Click the **Start** button and enter and click **firewall.cpl** in the search bar. Click **Turn Windows Firewall on or off** and then select **Turn off Windows Firewall** for **Domain network location settings, Home or work (private) network location settings and Public network location settings**. Click **OK**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Install the Configuration Manager Client | * + - 1. Once the system has joined the domain, log on to **CM1** virtual machine.       2. Launch the Configuration Manager Console and navigate to **Administration > Hierarchy Configuration >Discovery Methods**.       3. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt.       4. Navigate to **Assets and Compliance >** **Devices** and check if **WIN7** is showing in the list of devices.       5. Right-click on **WIN7** and click on **Install Client**       6. (hold Ctrl and select multiple computers if you want to install on more than one computer).       7. On the Install Configuration Manager Client wizard click on **Next**.       8. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**.       9. Click **Next** again.       10. Click on **Close**.       11. After a few minutes, the **WIN7** client will have the client installed and will indicate so in the Configuration Manager console.   **Note:** If by any chance the client fails to install, retry the installation after fully patching the machine. |
| **Complete these steps on the WIN7 virtual machine.** | |
| Create Checkpoint | * + - 1. Create a virtual machine **checkpoint**. |

#### Build a Windows 10 20H2 Client Machine

**Note:** The **WIN10** VM, will be used for the following scenarios in this Lab Guide:

* Section 4.4 - Servicing Windows 10 with Configuration Manager
* Section 9.2 - Windows App Certification Kit

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Hyper-V Host and the New Generation 2 virtual machine.** | |
| Create the Virtual Machine | 1. On the Hyper-V Host server, launch **Hyper-V Manager**. 2. Under **Actions**, click **New > Virtual Machine**. 3. On the **Before You Begin** page, click **Next**. 4. On the **Specify Name and Location** page, provide a Name (e.g. **WIN10-20H2**). Based on where you want to store virtual machine files, click **Store the virtual machine in a different location** and **Browse** to that specific location. Click **Next**. 5. On the **Specify Generation** page, select **Generation 2** and click **Next**. 6. On the **Assign Memory** page, provide a Startup memory of **2048 MB** or more and click **Next**. 7. On the **Configure Networking** page, in the Connection drop-down, select **HYD-CorpNet** and click **Next**. 8. On the **Connect Virtual Hard Disk** page, keep the defaults and click **Next**. 9. On the **Installation Options** page, select **Install an operating system from a bootable image file** and **Browse** to the ISO image as stated in **Steps 5-8** of **Section 2.3.5.1**. 10. On the **Summary** page, review and click **Finish**. 11. Click **Start** to turn on the VM and proceed with the installation. Join the system to the **corp.contoso.com** domain using the domain administrator credentials (**corp\labadmin**). 12. Log in as **CORP\LabAdmin** and then turn off the **Windows Defender Firewall Mode** for **Domain networks, Private networks and Guest or public networks**. Right-click on the **Start** button, click **Run** and enter **firewall.cpl**. Click **Turn Windows Defender Firewall on or off** and then select **Turn off Windows Defender Firewall** for **Domain networks, Private networks and Guest or public networks**. Click **OK**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Install the Configuration Manager Client | 1. Once the system has joined the domain, log on to **CM1** virtual machine. 2. Launch the Configuration Manager Console and navigate to **Administration > Hierarchy Configuration >Discovery Methods**. 3. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt. 4. Navigate to **Assets and Compliance >** **Devices** and check if **WIN10-20H2** is showing in the list of devices. 5. Right-click on **WIN10-20H2** and click on **Install Client** (hold Ctrl and select multiple computers if you want to install on more than one computer). 6. On the Install Configuration Manager Client wizard click on **Next**. 7. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**. 8. Click **Next** again. 9. Click on **Close**. 10. After a few minutes, the **WIN10-20H2** client will have the client installed and will indicate so in the Configuration Manager console.   **Note:** If by any chance the client fails to install, retry the installation. |
| **Complete these steps on the WIN10-20H2 virtual machine.** | |
| Create Checkpoint | 1. Create a virtual machine **checkpoint**. |

#### Build a Windows 10 21H1 Client Machine

In the activity, you will build Windows 10 21H1client virtual machine.

**Note:** The **WIN10-21H1** VM, will be used for the following scenarios in this Lab Guide:

* Section 3.1 - Desktop Analytics

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Hyper-V Host and the New Generation 2 virtual machine.** | |
| Create the Virtual Machine | 1. On the Hyper-V Host server, launch **Hyper-V Manager**. 2. Under **Actions**, click **New > Virtual Machine**. 3. On the **Before You Begin** page, click **Next**. 4. On the **Specify Name and Location** page, provide a Name (e.g. **WIN10-21H1**). Based on where you want to store virtual machine files, click **Store the virtual machine in a different location** and **Browse** to that specific location. Click **Next**. 5. On the **Specify Generation** page, select **Generation 2** and click **Next**. 6. On the **Assign Memory** page, provide a Startup memory of **2048 MB** or more and click **Next**. 7. On the **Configure Networking** page, in the Connection drop-down, select **HYD-CorpNet** and click **Next**. 8. On the **Connect Virtual Hard Disk** page, keep the defaults and click **Next**. 9. On the **Installation Options** page, select **Install an operating system from a bootable image file** and **Browse** to the ISO image as stated in **Steps 9-12** of **Section 2.3.5.1**. 10. On the **Summary** page, review and click **Finish**. 11. Click **Start** to turn on the VM and proceed with the installation. Join the system to the **corp.contoso.com** domain using the domain administrator credentials (**corp\labadmin**). 12. Log in as **CORP\LabAdmin** and then turn off the **Windows Defender Firewall Mode** for **Domain networks, Private networks and Guest or public Networks**. Right-click on the **Start** button, click **Run** and enter **firewall.cpl**. Click **Turn Windows Defender Firewall on or off** and then select **Turn off Windows Defender Firewall** for **Domain networks, Private networks and Guest or public Networks**. Click **OK**. 13. Install the **latest Compatibility/Cumulative Updates**. You must reboot the VM multiple times and check for any remaining updates to be installed until no further updates are required. This step is important for the **Desktop Analytics scenario**. Click **Start > Settings > Update & Security > Check for updates**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Install the Configuration Manager Client | 1. Log on to **CM1** virtual machine. 2. Launch the Configuration Manager Console and navigate to **Administration > Hierarchy Configuration >Discovery Methods**. 3. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt. 4. Navigate to **Assets and Compliance >** **Devices** and check if **WIN10-21H1** is showing in the list of devices. 5. Right-click on **WIN10-21H1** and click on **Install Client** (hold Ctrl and select multiple computers if you want to install on more than one computer). 6. On the Install Configuration Manager Client wizard click on **Next**. 7. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**. 8. Click **Next** again. 9. Click on **Close**. 10. After a few minutes, the **WIN10-21H1** client will have the client installed and will indicate so in the Configuration Manager console.   **Note:** If by any chance the client fails to install, retry the installation. |
| **Complete these steps on the WIN10-21h1 virtual machine.** | |
| Create Checkpoint | 1. Create a virtual machine **checkpoint**.   **Note:** Repeat **Steps 14-23** above to install the Configuration Manager Client on **HYD-CLIENT1**, **HYD-CLIENT2** and **HYD-CLIENT7**. If by any chance the client fails to install, retry the installation.  **Note:** The **Windows Defender Firewall Mode** for **Domain networks, Private networks and Guest or public Networks** must be turned off on **HYD-CLIENT1-7**. Refer to **Step 12** above.  **Note:** For the **Desktop Analytics scenario**, the **Windows Defender Firewall Mode** must be turned off for **Domain networks, Private networks and Guest or public Networks** in the following VMs in the lab - **DC1, CM1, GW1, Windows 10 21H1 VM and your Hyper-V Host**. This is to ensure that there are no blocks in the data flow from the lab to Azure. Refer to **Step 12** above.  **Note:** For **HYD-Client5** and **HYD-Client6**, ensure that they must be assigned **2048 MB or more of Memory** and atleast **2 vCPUs** and create new **Checkpoints** for each. |

#### Build a Windows 10 Developer Machine

In this activity, you will build Windows 10 client virtual machine with developer tools installed.

**Note:** The **WIN10DEV** VM, will be used for the following scenarios in this Lab Guide:

* Section 9.2 - Windows App Certification Kit

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows Server with Hyper-V enabled computer.** | |
| Download Developer VM (if not previously downloaded) | 1. Open **File Explorer** and create the **C:\VMs** folder. 2. Open **Internet Explorer** and browse to the **URL** below.   <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines>   1. Under **Windows 10 Enterprise - 20 GB download**, click **Hyper-V**. 2. Download **WinDev2005Eval.HyperVGen1.zip** to **C:\VMs**. 3. Once the download completes, browse to **C:\VMs**, right-click on **WinDev2005Eval.HyperVGen1.zip** and select **Extract All**. 4. In the **Select a Destination and Extract Files** page, click **Extract**. |
| Import VMs | 1. Open **File Explorer** and create the **C:\VMs\WIN10DEV** folder. 2. Open **Hyper-V Manager**. 3. In the **Actions** pane, click **Import Virtual Machine**. 4. In the **Before You Begin** page, click **Next**. 5. In the **Locate Folder** page, browse to **C:\VMs\WinDev2005Eval.HyperVGen1\** then click **Next**. 6. In the **Select Virtual Machine** page, click **Next**. 7. In the **Choose Import Type** page, select **Copy the virtual machine** then click **Next**. 8. In the **Choose Destination** page, select **Store the virtual machine in a different location**, enter the path **C:\VMs\WIN10DEV\** to all folders then click **Next**. 9. In the **Choose Storage Folder** page, enter the path **C:\VMs\WIN10DEV\** then click **Next**. 10. In the **Summary** page, click **Finish**. 11. In the **Hyper-V Manager**, right-click on **WinDev2005Eval**, select **Rename** and enter **WIN10DEV**. |
| **Complete these steps on the WIN10DEV virtual machine.** | |
| Configure Virtual Machine Settings | 1. In the **Hyper-V Manager**, right-click on **WIN10DEV** and select **Settings**. 2. Configure the following then click **OK**.   **Memory**: 8192  **Processor**: 4 virtual processors  **Network Adapter**: **HYD-CorpNet**   1. **Start** the **WIN10DEV** virtual machine. |
| Install Windows Updates | 1. Go to **Start** and click **Settings**. 2. In the **Settings** app, browse to **Update & Security > Windows Update**. 3. Click **Check for updates** or **Retry** if they are in failed state. 4. **Install** all missing updates (restart if needed) until the device is **up to date**.   **Note**: This may take at least an hour depending on the internet speed. |
| Perform Defender Scan | 1. In the **Settings** app, browse to **Update & Security > Windows Security**. 2. Click **Open Windows Security**. 3. Click **Virus & threat protection**. 4. Click **Quick scan**. 5. Once complete, close **Windows Security** and the **Settings** app. |
| Create Checkpoint | 1. Create a virtual machine **checkpoint**. |

## Cloud Environment Set Up

### Configuration

Follow the steps below to configure and prepare the required cloud services.



#### Azure AD and Microsoft 365

In this section, you will create an Azure AD and a Microsoft 365 Trial Tenant used for the later lab environment.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Azure AD | **Note:** If Azure AD is already present and associated with a Subscription, then skip this section.   1. Open an InPrivate Browser session. 2. Navigate to <https://portal.azure.com> 3. Sign in with the **email address** associated with your Azure subscription. 4. On the left navigation bar, click **Create a resource > Identity > Azure Active Directory**. 5. Click **Create.** 6. In the Create directory pane fill in the following values:   ORGANIZATION NAME: **<CompanyName>**  INITIAL DOMAIN NAME: **<AzureDomainName>**  COUNTRY OR REGION: **Choose a region**   1. Click **Create**.   **Note**: This may take a couple of minutes to complete. |
| Create Azure AD Admin User | 1. Sign out from Azure portal and sign back in again. 2. Click your **email address** on the upper right corner and click **Switch directory**. Select **<AzureDomainName>.onmicrosoft.com**. If required, refresh the page for the directory to be visible. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Users** and then click **+ New user**. 5. In the New user pane, fill in the following values:   USER NAME: **<LabAdmin>** (Suggestion: LabAdmin@<AzureDomainName>.onmicrosoft.com)  NAME: **<Admin Name>**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name   1. Select **Auto-generate password** and select **Show Password** and write down the temporary password **<OldLabAdminPassword>**. 2. Click on **User** next to **Roles**, select **Global administrator** and **Desktop Analytics administrator**, then click **Select**.   **Note:** The Desktop Analytics administrator role is required here for the Desktop Analytics scenario only, NOT for the Windows Virtual Desktop scenario.   1. Click **Create**. |
| Resetting the Password | 1. Logout from Azure Portal. 2. Log in to Azure Portal using **LabAdmin** account. 3. Type in the **<OldLabAdminPassword>** that you wrote down. 4. Type the new password: **<NewLabAdminPassword>**. 5. Confirm the new password and sign in. |
| Associate a Subscription with the New Azure AD Tenant | **Note**: If Azure AD is already present and associated with a Subscription, then skip this section.   1. Click **All services > Subscriptions**. 2. Click **Add** to add a new subscription to the new Azure AD Tenant. 3. If you are eligible for a Free Trial, then click **Free Trial** or select any other offer from the list. 4. Follow the instructions for **Azure – Sign up**. 5. At the end you must be able to see a valid Active Subscription with a Subscription ID in the **All services > Subscriptions** pane. |
| Subscribe to Microsoft 365 E3 Trial Subscription | 1. Open a new tab and navigate to <https://portal.office.com>. 2. Click the **Admin** tile. 3. Click **Billing | Purchase services**. 4. Search for and select **Microsoft 365 E3** and then click **Get free trial**. 5. Follow the usual procedure for verification and click **Try now | Continue**. You should now be able to see the subscription under **Billing | Your products**. |
| Create Azure Test Users | 1. Navigate to <https://portal.azure.com>. 2. Sign in with the email address associated with your Azure subscription if required. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Add** and then click **+ New user**. 5. In the New user pane, fill in the following values:   USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**  NAME: **Test User1**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name   1. Select **Let me create the password** and enter **P@ssw0rd**. 2. Click **Add.** 3. Repeat **Steps 89-91** for a second user as follows:   USER NAME: **TU2@<AzureDomainName>.onmicrosoft.com**  NAME: **Test User2**  FIRST NAME: Enter the first name  LAST NAME: Enter the last name |
| Create Azure AD Group (Sales) | 1. Open an InPrivate Browser session. 2. Navigate to <https://portal.azure.com> 3. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 5. Click **+ New group**. 6. In the New Group pane fill in the following values:   Group type: **Microsoft 365**  Group name: **Sales**  Membership type: **Assigned**  Members: **Test User1** and **Test User2**   1. Click **Create**. |

#### Enable and Configure Cloud Licenses

In the section, you will assign licenses and configure additional cloud services that will be used in the lab environment.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Assign Microsoft 365 E3 and EM+S Licenses | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.office.com> and **Sign in** with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. Click on Azure services>**Azure Active Directory**. 5. On left nav, click **Licenses.** 6. On right nav, click **Get a free trial.** 7. On Enterprise Mobility + Security E5, click **Activate**. Close box. 8. On right nav, click **Manage your purchased licenses**. 9. In Products, check **Enterprise Mobility + Security E5** and click **+Assign.** 10. Click **+Add users and groups.** Click on each user (admin, TU1, TU2) to assign licenses. Click **Select.** 11. Click **Review + assign** to ensure that all the 3 users have all the product licenses assigned. |
| Enable Device Registration | 1. Close all browser windows. 2. Open an **InPrivate Browser** session. 3. Navigate to <https://portal.azure.com>. 4. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 5. Click **Azure Active Directory > Devices > Device settings**. 6. In the **Users may join devices to Azure AD** setting, select **All** if not selected. |
| Enable Windows Defender ATP Trial | **Note**: A trial application should have been started before proceeding with the steps - <https://www.microsoft.com/en-us/windowsforbusiness/windows-atp>   1. Close all browser windows. 2. Open an InPrivate Browser session. 3. Navigate to <https://www.microsoft.com/en-us/windowsforbusiness/windows-atp> and click **Start free trial**. 4. Check the box next to **I accept these terms and conditions** and click **Next**. 5. On the Please enter your details below page, enter your details and click **Submit**. 6. You will get a message stating that the Windows Defender Advanced Threat Protection Team will review your application and contact you via email within 7 business days. Once your application is approved, you will then receive an invitation email with onboarding instructions. 7. Within 7 business days, you will then receive an email to activate your trial and all the onboarding instructions. Click **Activate your trial now**. Download the **setup guide**. The setup guide also contains instructions and links for the attack demo. 8. During activation, click **Sign in**. 9. **Sign in** with **LabAdmin@<AzureDomainName>.onmicrosoft.com** 10. Click **Try now**. 11. Click **Continue**. 12. Close all browser windows. |

#### Configure Azure AD Connect with Device Sync

In this activity, you will configure Azure AD Connect on DC1.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| **Configure Azure AD Connect** | 1. Click **Start > Windows Administrative Tools > Active Directory Domains and Trusts**. Right-click **Active Directory Domains and Trusts** and click **Properties**. In the **UPN Suffixes** tab, enter **<AzureDomainName>.onmicrosoft.com** and remove **contoso.com**. Click **Add** and click **Apply** and **OK**. 2. Click **Start > Windows Administrative Tools > Active Directory Users and Computers**. 3. Navigate to **corp.contoso.com > Users** and double-click **LabAdmin**. Click the **Account** tab and under **User logon name**, enter **LabAdmin** and in the drop down select **<AzureDomainName>.onmicrosoft.com**. Click **Apply** and **OK**. 4. Download **Azure AD Connect** from <https://www.microsoft.com/en-us/download/details.aspx?id=47594> 5. Run **Azure AD Connect** and select **I agree to the license terms and privacy notice** and click **Continue**. Accept the UAC prompt. 6. Select **Use express settings**. 7. In the **Connect to Azure AD** prompt, sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 8. In the **Connect to AD DS** prompt enter the following and click **Next**. USERNAME: **CORP\LabAdmin** PASSWORD: **P@ssw0rd** 9. On the **Azure AD sign-in configuration** page, ensure that the UPN suffix added in **Step 1** is listed and then select **Continue without matching all UPN suffixes to verified domains** and click **Next**. 10. On the **Ready to configure** page, keep the checkbox checked next to **Start the synchronization process when configuration completes** and click **Install**. Click **Exit** once synchronization is complete. |
| **Configure Device Sync** | 1. Open **Apps and Features** and uninstall the **Windows Azure Active Directory Module for Windows PowerShell**. Accept the UAC prompt. 2. Open PowerShell as an administrator. Accept the UAC prompt. 3. Create a directory in **C drive**, example **C:\MSOnline**. 4. Run the below cmdlet and accept any prompts. Save-Script -Name MSOnline -Path C:\MSOnline\ 5. Run the below cmdlet and accept any prompts. Install-Module -Name MSOnline 6. Locate the name of the **AAD Connector Account** by opening the **Azure AD Connect** and clicking **Configure** and selecting **View or export current configuration** and then clicking **Next**. Click **Exit**. 7. Run the below cmdlet and at the credential prompt, provide the Azure AD Admin credentials. Import-Module -Name “C:\Program Files\Microsoft Azure Active Directory Connect\ADPrep\ADSyncPrep.psm1”   $aadadmincred = get-credential;  Initialize-ADSyncDomainJoinedComputerSync -AdConnectorAccount <account name> -AzureADCredentials $aadAdminCred; |
| **Confirm Devices are Hybrid Azure AD Joined** | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 3. On the left navigation bar, click **Azure Active Directory**. 4. Select **Devices** > **All devices**. 5. Confirm devices are registered to Azure AD.   **Note:** In case the On-Prem Domain-Joined Clients do not show up in Azure AD, perform the following steps:   1. Disable the firewall mode in **DC1** if not done already. 2. Open **Azure AD Connect** and click **Configure**. 3. Select **Configure device options** and click **Next**. 4. Click **Next** again. 5. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 6. Select **Configure Hybrid Azure AD join** and click **Next**. 7. Select **Windows 10 or later domain-joined devices** and click **Next**. 8. Check the box next to **corp.contoso.com** and click **Add**. 9. Sign in with **CORP\LabAdmin** and **P@ssw0rd** and click **OK**. 10. Click **Next**. 11. Click **Configure**. 12. Click **Exit** once done. 13. Open **Azure AD Connect** and click **Configure**. 14. Select **Customize synchronization options** and click **Next**. 15. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 16. Click **Next** again. 17. Click **Next** again. 18. Ensure that **Password hash synchronization** is selected. Also select **Password writeback** and click **Next**. 19. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done. 20. Open **Azure AD Connect** and click **Configure**. 21. Select **Change user sign-in** and click **Next**. 22. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 23. Select **Pass-through authentication** and ensure that **Enable single sign-on** is selected and then click **Next**. 24. Click **Enter credentials** and enter **CORP\LabAdmin** and **P@ssw0rd**. Click **OK**. Click **Next**. 25. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done. 26. Follow **Steps 16-20** above specially to confirm the On-Prem Domain-Joined Clients show up in Azure AD. Please note, it may take some time (15-30 minutes) for the machines to appear in the console.   **Note:** Log in to any **Windows 10 Enterprise Version 21H1 VM** as **labadmin@<AzureDomainName>.onmicrosoft.com** with the password **P@ssw0rd**.  On the client side, the **dsregcmd /status** command will give the following results to determine that the device is Hybrid Azure AD Joined. For more information, refer to <https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>:      **Note:** If the clients are showing **Pending** under the **Registered** column in the Azure Portal for a long time, to instantly register, run the command **dsregcmd /join** from the client side. |

# Plan and Prepare Infrastructure

## Desktop Analytics

Desktop Analytics is a cloud-based service that integrates with Configuration Manager. The service provides insight and intelligence for you to make more informed decisions about the update readiness of your Windows clients. It combines data from your organization with data aggregated from millions of devices connected to Microsoft cloud services.

Use Desktop Analytics with Configuration Manager to:

* Create an inventory of apps running in your organization.
* Assess app compatibility with the latest Windows 10 feature updates.
* Identify compatibility issues, and receive mitigation suggestions based on cloud-enabled data insights.
* Create pilot groups that represent the entire application and driver estate across a minimal set of devices.
* Deploy Windows 10 to pilot and production-managed devices.

**Note:** Desktop Analytics is a successor of Windows Analytics. The Windows Analytics service includes Upgrade Readiness, Update Compliance, and Device Health. All of these capabilities are combined in the Desktop Analytics service. Desktop Analytics also is more tightly integrated with Configuration Manager.

For more information, refer to [https://docs.microsoft.com/en-us/configmgr/desktop-analytics/overview](https://docs.microsoft.com/en-us/sccm/desktop-analytics/overview) and every sub-section of this article.

### Desktop Analytics – Prerequisites

The following are required to run the Desktop Analytics in the lab environment:

On-premises environment

1. **One or more** **user-provisioned Windows 10 21H1 EVAL client VMs.** The Windows 10 **21H1** EVAL client VMs must be fully updated and patched with the latest Windows 10 Compatibility/Cumulative Updates. It must also have the latest version of the Configuration Manager client installed. We have used one **21H1** client VM for this lab. For set-up guidance, see:
2. Section 2.3.5.1- Download Windows 10 21H1 ISO EVAL
3. Section 2.3.5.3- Build a Windows 10 21H1 Client Machine

**IMPORTANT NOTE: The Desktop Analytics scenario requires manually provisioned client virtual machines. The client VMs that come pre-installed in the lab environment should not be used as they may not generate the telemetry needed for the Desktop Analytics lab.**

1. **The latest version of Configuration Manager**. This scenario has been tested with Configuration Manager 2010. You must be logged into CM1 with the CORP\LabAdmin account which has the Full Administrator role. For set-up guidance, see:
2. Section 2.3.2 - Configure as Online Mode
3. Section 2.3.4 - Prepare Configuration Manager (if not already configured)
4. **Windows Defender Firewall Mode adjustment.** The firewall must be turned off for Domain networks, Private networks and Guest or public Networks in the following VMs in the lab - DC1, CM1, GW1, Windows 10 21H1 VM and your Hyper-V Host. This is to ensure that there are no blocks in the data flow from the lab to Azure.

**Note:** If you have a proxy in your network on which you are running your host machine, you will need to configure your proxy server to allow specific endpoints. For all endpoints required for this scenario and other setup guidance, see:

1. [Enable data sharing for Desktop Analytics – Endpoints](https://docs.microsoft.com/en-us/configmgr/desktop-analytics/enable-data-sharing#endpoints)
2. Section 2.3.5.4 - Create the Virtual Machine

Cloud environment

1. **Active Azure Subscription with Global Admin permissions.** For this lab, this user needs to also have the Desktop Analytics Administrator role manually assigned. For set-up guidance, see:
2. Section 2.2.1 – Set up Azure and Microsoft 365
3. **Microsoft 365 E3 Trials.** Licenses for these subscriptions must be assigned to [labadmin@<AzureDomainName>.onmicrosoft.com](mailto:labadmin@%3cAzureDomainName%3e.onmicrosoft.com). For set-up guidance, see:
4. Section 2.2.1 - Set up Azure and Microsoft 365
5. Section 2.2.3 – Enable and Configure Cloud service - (Ignore other users created for other labs and also ignore EM+S Licenses as part of this sub-section)

### Set up Desktop Analytics in Azure

Use this procedure to sign into Desktop Analytics and configure it with your Microsoft 365 subscription in Azure. This procedure is a one-time process to set up Desktop Analytics for your organization.

For more information, refer to [https://docs.microsoft.com/en-us/configmgr/desktop-analytics/set-up](https://docs.microsoft.com/en-us/sccm/desktop-analytics/set-up)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Set up Desktop Analytics | 1. On the Microsoft 365 Device Management portal, open the Desktop Analytics portal at: <https://aka.ms/desktopanalytics>. Sign in as the user set up previously with the Global Admin role (**labadmin@<AzureDomainName>.onmicrosoft.com**). Click **Start** to start setting up Desktop Analytics. 2. On the **Accept service agreement** page, review the service agreement, and select **Accept**. 3. On the **Licensing and costs** page, review the list of required qualifying licenses. Switch the setting to **Yes** next to **Do you have one of the supported subscriptions?**, and then select **Next**. 4. On the **Give users and apps access** page, do the following and select **Next**: 5. **Directory role management** - **Allow Desktop Analytics to manage Directory roles on your behalf** - Ensure it is switched to **Yes**. 6. **Workspace owners** - Ensure **LabAdmin** is already listed. 7. On the **Set up your workspace** page, do the following: 8. **Select an Azure subscription** - Select your subscription from the drop-down. 9. Now to create a workspace for Desktop Analytics, select **Add workspace**. 10. Enter a globally unique **Workspace name**. 11. Select the drop-down list to **Select the Azure subscription for this workspace**, and choose the Azure subscription for this workspace. 12. Select **Create new** under **Resource group** and provide a unique name for the resource group. 13. Under **Select the region closest to your organization**, select the appropriate region and then select **Add**. 14. Select the Workspace added and then select **Set as Desktop Analytics workspace**. Then select **Continue** in the **Confirm and grant access** dialog. 15. In the new browser tab, pick an account to use to sign in (**labadmin@<AzureDomainName>.onmicrosoft.com**). Select the option to **Consent on behalf of your organization** and select **Accept**. 16. Back on the page to **Set up your workspace**, select **Next**. 17. On the **Next steps** page, select **Go to Desktop Analytics**. The Azure portal shows the Desktop Analytics **Home** page with a message **"Welcome to Desktop Analytics! You will need to enroll devices in Configuration Manager to populate your workspace."** |

### Connect Configuration Manager with Desktop Analytics

Use this procedure to connect Configuration Manager to Desktop Analytics, and configure device settings. This procedure is a one-time process to attach your hierarchy to the cloud service. For more information, refer to [https://docs.microsoft.com/en-us/configmgr/desktop-analytics/connect-configmgr](https://docs.microsoft.com/en-us/sccm/desktop-analytics/connect-configmgr)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Connect Configuration Manager with Desktop Analytics | 1. Log in to **CM1** as **CORP\LabAdmin** and launch the Configuration Manager console. 2. In the Configuration Manager console, go to **Assets and Compliance > Device Collections**. 3. Right-select **Device Collections** and select **Create Device Collection**. 4. On the **General** page, provide a **Name**, example: **DALabCollection** and select **Browse**. 5. Under **Device Collections | Root**, select **All Systems** and select **OK**. Select **Next**. 6. On the **Membership Rules** page, select **Add Rule > Direct Rule**. Select **Next**. In the **Value** field, search the name of the Windows 10 21H1 Client VM, example **%WIN10-21H1%** and select **Next**. Select the machine from the results and select **Next**. Select **Next**. Select **Close**. 7. On the **Membership Rules** page, select **Next**. 8. On the **Summary** page, select **Next**. 9. On the **Completion** page, select **Close**. 10. Ensure that machine shows up in the collection. 11. Now go to the **Administration** workspace, expand **Cloud Services**, and select the **Azure Services** node. Select **Configure Azure Services** in the ribbon. 12. On the **Azure Services** page of the Azure Services Wizard, configure the following settings and select **Next**: 13. Specify a **Name** for the object in Configuration Manager. 14. Specify an optional **Description** to help you identify the service. 15. Select **Desktop Analytics** from the list of available services. 16. On the **App** page, select the appropriate **Azure environment (AzurePublicCloud)**. Then select **Browse** for the web app. 17. On the **Server App** window, select **Create**. 18. Configure the following settings in the **Create Server Application** window: 19. **Application Name**: A friendly name for the app in Azure AD. 20. **HomePage URL**: This value isn't used by Configuration Manager, but required by Azure AD. By default this value is **https://ConfigMgrService**. But you may change the value here to make it unique. 21. **App ID URI**: This value needs to be unique in your Azure AD tenant. It's in the access token used by the Configuration Manager client to request access to the service. By default this value is **https://ConfigMgrService**. But you may change the value here to make it unique. 22. **Secret Key validity period**: Choose either **1 Year or 2 Years** from the drop-down list. **1 Year** is the default value. 23. Select **Sign in**. After successfully authenticating to Azure, the page shows the **Azure AD Tenant Name** for reference. 24. Select **OK** to create the web app in Azure AD and close the **Create Server Application** window. 25. On the **Server App** window, select the app and select **OK**. Then select **Next** on the **App** page of the Azure Services Wizard. 26. On the **Diagnostic Data** page, configure the following settings and select **Next**: 27. **Commercial ID**: This value should automatically populate with your organization's ID. If it doesn't, make sure your proxy server (if you have one in your location) is configured to allow all required endpoints before continuing. Alternatively, you can retrieve your Commercial ID manually from the Desktop Analytics portal. 28. **Windows 10 diagnostic data level**: Select **Enhanced**. 29. **Allow Device Name in diagnostic data**: Select **Enable**. 30. The **Available Functionality** page shows the Desktop Analytics functionality that's available with the diagnostic data settings from the previous page. Select **Next** to continue. 31. On the **Collection** page, configure the following settings and select **Next**: 32. **Display Name**: The Desktop Analytics portal displays this Configuration Manager connection using this name. Use it to differentiate between different hierarchies. For example, **DALab**. 33. **Target Collection**: This collection includes all devices that Configuration Manager configures with your commercial ID and diagnostic data settings. It's the full set of devices that Configuration Manager connects to the Desktop Analytics service. Over here, select **Browse** and select the collection created above in **Steps 2-10**. Select **OK**. 34. **Devices in the target collection use a user-authenticated proxy for outbound communication**: By default, this value is **No**, so keep the default value. 35. In the **Select additional collections to use with deployment plans. Make sure to include pilot and pilot exclusion collections**, leave blank for this scenario. 36. On the **Summary** page, select **Next**. 37. On the **Completion** page, select **Close**. |

### Monitor Connection Health

Use the **Connection Health** dashboard in Configuration Manager to drill down into categories by device health.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Windows 10 21H1 Client virtual machine.** | |
| Trigger diagnostic settings on client VM (Optional) | **Note:** After connecting Configuration Manager to Desktop Analytics, the clients will automatically begin to send data to Desktop Analytics. After set-up, clients update policy every hour. You can trigger policy updates by following these steps:   1. In the **Control Panel**, go to **System and Security>Configuration Manager** to open the **Configuration Manager client applet.** 2. Click on the **Actions** tab and run all actions one by one. 3. On the **Configurations** tab, notice the **M365ASettings** policy to configure the device in the Target Collection. This policy includes the diagnostic data settings to enable the device to send data to Microsoft. 4. Click on **M365ASettings** and select **Evaluate** and **Refresh.** Close the applet. 5. Go to **C:\Windows\CCM\logs** to open the **M365AHandler.log** for details of when the data has been sent to Microsoft for getting processed.   **Note: After triggering the policies, it can be several hours or more (up to 72 hours)**  **for active devices to send diagnostic data to the Desktop Analytics service and for** **the service to process the data, and then synchronize with your Configuration Manager site.** |
| **Complete these steps on the CM1 virtual machine.** | |
| Monitor Connection Health | 1. In the **Configuration Manager console**, go to the **Software Library** workspace, expand the **Desktop Analytics Servicing** node, and select the **Connection Health** dashboard. Use the Connection Health dashboard to drill down into categories by device health.   **Note**: When you first set up Desktop Analytics, it may take up to 72 hours for these charts to show complete client data. The following example screen shows a scenario with complete data for multiple clients.  Screenshot of the Configuration Manager Connection Health dashboard |

## Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP)

The Cloud Management Gateway (CMG) provides a simple way to manage Configuration Manager clients on the Internet. By deploying the CMG as a cloud service in Microsoft Azure, you can manage traditional clients that roam on the Internet without additional infrastructure. You also don't need to expose your on-premises infrastructure to the internet.

A Cloud Distribution Point (CDP) is a Configuration Manager distribution point that is hosted as Platform-as-a-Service (PaaS) in Microsoft Azure. This service supports the following scenarios:

1. Provide software content to Internet-based clients without additional on-premises infrastructure.
2. Cloud-enable your content distribution system.
3. Reduce the need for on-premises distribution points.

This section provides the steps to install and configure the Cloud Management Gateway (CMG) along with the Cloud Distribution Point (CDP).

**Note:** Ensure that a trial subscription has been associated with the previously created **<AzureDomainName>.onmicrosoft.com**.

**Note:** The **Microsoft.ClassicCompute** and **Microsoft.Storage** resource providers must be registered within the Azure subscription. To verify that in the Azure portal, click **All services | search for and click Subscriptions | click the subscription | Resource providers**. If not registered, click **Register** for **Microsoft.ClassicCompute** and **Microsoft.Storage**.

**Note:** For more information, refer to <https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/setup-cloud-management-gateway>

### Check for the Globally Unique Name

Before setting up and configuring the CMG server authentication certificate, it is required to know a globally unique name for the service that will be configured in the CMG server authentication certificate. To do so, perform the following steps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Check for the Globally Unique Name | 1. Log into the Azure portal using the **labadmin@<AzureDomainName>.onmicrosoft.com** account. 2. Click **Create a resource** from the top left-hand corner. 3. In **Search the Marketplace** search box, type **Cloud Service** and select **Cloud Service** from the search results. 4. Click **Create** in the **Cloud service** blade. 5. In **DNS name**, type a globally unique name and ensure it is available. 6. In **Subscription**, select the appropriate subscription. 7. In **Resource group**, select **Create new** and type in the name of a resource group not already in use. Click **OK**. 8. In **Location**, select the appropriate location which is supported by the subscription. 9. Ensure that there are no errors on the **Cloud service (classic)** blade, take a note of all the details and exit.   **Note:** Do not create the cloud service. |

### Create and Issue the CMG Server Authentication Certificate

After the globally unique name for the service is known, create and issue the CMG server authentication certificate by performing the following steps.

**Note:** In **DC1**, Active Directory, create a Security Group, example **ConfigMgr Site Servers** and add **CM1** into this Security Group.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Create and Issue the CMG Server Authentication Certificate | 1. Launch the **Certification Authority** console. 2. Right-click **Certificate Templates**, and then click **Manage** to load the Certificate Templates console. 3. In the Certificate Templates console, right-click the entry that has **Web Server** in the Template Display Name column, and then click **Duplicate Template**. 4. In the Properties of New Template window, ensure that **Windows Server 2003** is selected under **Certification Authority** and **Windows XP / Server 2003** is selected under **Certificate recipient**. 5. On the **General** tab, enter a template name, example: **CMG Server Authentication Certificate**, to generate the web server certificate for CMG. 6. Click the **Request Handling** tab, and then select **Allow private key to be exported**. 7. Click the **Security** tab, and then remove the **Enroll** permission from the **Enterprise Admins** security group. 8. Click **Add**, enter the name of the security group, example: **ConfigMgr Site Servers** that contains the computer object of the ConfigMgr site server in the text box, and then click **OK**. 9. Select the **Enroll** permission for the security group, example: **ConfigMgr Site Servers**, and “do not” clear the **Read** permission checkbox. 10. Click **OK**, and then close the Certificate Templates console. 11. Back in the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**. 12. In the Enable Certificate Templates window, select the new template configured, example: **CMG Server Authentication Certificate**, and then click **OK**. Close the Certification Authority console. |

### Request the CMG Server Authentication Certificate

After the CMG server authentication certificate is created and issued, request this certificate on **CM1** by performing the following steps.

**Note:** Reboot **CM1** once, so that the server can access the certificate template using the Read and Enroll permissions.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Request the CMG Server Authentication Certificate | 1. Right-click **Start**, click **Run**, enter **mmc** and press enter. Accept the UAC prompt. In the empty console, click **File**, and then click **Add/Remove Snap-in**. 2. In the Add or Remove Snap-ins window, select **Certificates** from the list of Available snap-ins, and then click **Add**. 3. In the Certificate snap-in window, select **Computer account**, and then click **Next**. 4. In the Select Computer window, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. 5. In the Add or Remove Snap-ins window, click **OK**. 6. In the console, expand **Certificates (Local Computer)**, and then click **Personal**. 7. Right-click **Certificates**, click **All Tasks**, and then click **Request New Certificate**. 8. On the Before You Begin page, click **Next**. 9. On the Select Certificate Enrollment Policy page, click **Next**. 10. On the Request Certificates page, identify the certificate, example: **CMG Server Authentication Certificate** from the list of available certificates, and then click **More information is required to enroll for this certificate. Click here to configure settings.** 11. In the Certificate Properties window, in the **Subject** tab, for the **Subject name**, select **Common name** as the **Type**. 12. In the **Value** box, specify the globally unique name recorded in **Section 5.2.1**, in an FQDN format ending with **cloudapp.net**. 13. Click **Add** and then click **OK** to close the Certificate Properties dialog box. 14. Back in the Request Certificates page, select the certificate, example: **CMG Server Authentication Certificate** from the list of available certificates, and then click **Enroll**. 15. On the Certificates Installation Results page, wait until the certificate is installed, and then click **Finish**. 16. Verify that a new certificate has been created under **Personal | Certificates**. |

### Export the CMG Server Authentication Certificate

After the CMG server authentication certificate is requested in **CM1**, it needs to be exported by performing the following steps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Export the CMG Server Authentication Certificate | 1. In the Certificates (Local Computer) console, right-click the **certificate** that was just configured and enrolled, click **All Tasks**, and then click **Export**. 2. In the Certificate Export Wizard, click **Next**. 3. On the Export Private Key page, click **Yes, export the private key**, and then click **Next**. 4. On the Export File Format page, ensure that the **Personal Information Exchange - PKCS #12 (.PFX)** option is selected along with the option **Include all certificates in the certification path if possible** and **Enable certificate privacy** and then click **Next**. 5. On the Security page, specify a strong password to protect the exported certificate with its private key, and then click **Next**. 6. On the File to Export page, **Browse** to a suitable location to save the certificate, specify the name of the **PFX** file to be exported, and then click **Save | Next**. 7. To close the wizard, click **Finish** in the Certificate Export Wizard page, and then click **OK** in the confirmation dialog box. 8. Store the file securely and ensure that you can access it from the ConfigMgr console. This certificate will be required during setting up CMG. |

### Create and Issue the Client Authentication Certificate

To create and issue the client authentication certificate, perform the following steps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Create and Issue the Client Authentication Certificate | 1. Launch the **Certification Authority** console. 2. Right-click **Certificate Templates**, and then click **Manage** to load the Certificate Templates console. 3. In the Certificate Templates console, right-click the entry that has **Workstation Authentication** in the Template Display Name column, and then click **Duplicate Template**. 4. In the Properties of New Template window, ensure that **Windows Server 2003** is selected under **Certification Authority** and **Windows XP / Server 2003** is selected under **Certificate recipient**. 5. On the **General** tab, enter a template name, example: **ConfigMgr Client Authentication Certificate**, to generate the client certificates that will be used on ConfigMgr client computers. 6. Click the **Security** tab, select the **Domain Computers** group, and then select the additional permissions of **Read** and **Autoenroll**. Do not clear **Enroll**. 7. Click **OK**, and then close the Certificate Templates console. 8. Back in the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**. 9. In the Enable Certificate Templates window, select the new template configured, example: **ConfigMgr Client Authentication Certificate**, and then click **OK**. Close the Certification Authority console. |

### Configure Autoenrollment of the Client Authentication Certificate using Group Policy

After the client authentication certificate is created and issued, a group policy is configured to autoenroll the client authentication certificate to client computers by performing the following steps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure Autoenrollment of the Client Authentication Certificate using Group Policy | 1. Click **Start | Windows Administrative Tools | Group Policy Management**. 2. Right-click on the root of the domain, and then click **Create a GPO in this domain, and Link it here**. 3. In the New GPO dialog box, enter a name, example: **Client Authentication Certificate Autoenrollment**, and then click **OK**. 4. In the results pane, on the **Linked Group Policy Objects** tab, right-click the new group policy, and click **Edit**. 5. In the Group Policy Management Editor window, navigate to **Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies**. 6. Right-click **Certificate Services Client – Auto-Enrollment** and click **Properties**. 7. For the **Configuration Model**, select **Enabled**, select **Renew expired certificates, update pending certificates, and remove revoked certificates** and select **Update certificates that use certificate templates**. Click **OK**. 8. Close the Group Policy Management Editor and the console. |

### Automatically Enroll the Client Authentication Certificate and Verify its Installation

After configuring autoenrollment of the client authentication certificate using group policy, to automatically enroll the certificate and verify its installation, perform the following steps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Automatically Enroll the Client Authentication Certificate and Verify its Installation | 1. Reboot **CLIENT1** and run a **gpupdate /force**. Run a **gpupdate /force** on **CM1** as well. 2. Right-click **Start**, click **Run**, enter **mmc** and press enter. Accept the UAC prompt if required. In the empty console, click **File**, and then click **Add/Remove Snap-in**. 3. In the Add or Remove Snap-ins window, select **Certificates** from the list of Available snap-ins, and then click **Add**. 4. In the Certificate snap-in window, select **Computer account**, and then click **Next**. 5. In the Select Computer window, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. 6. In the Add or Remove Snap-ins window, click **OK**. 7. In the console, expand **Certificates (Local Computer) | Personal** and select **Certificates**. 8. In the results pane, confirm that the certificate is present that has **Client Authentication** in the **Intended Purposes** column, and that example: **ConfigMgr Client Authentication Certificate** is in the **Certificate Template** column. |

### Client Trusted Root Certificate to CMG

The CMG must trust the client authentication certificates. Client trusted root certificate to CMG is required when using client authentication certificate. When clients use Azure AD for authentication, then this certificate is not required. To accomplish this trust, provide the trusted root certificate chain by performing the following steps.

**Note:** It is not required to configure the other type of certificate called CMG Trusted Root Certificate to Clients in this lab because there is only one Trusted Root Certification Authority. Configuring the Client Trusted Root Certificate to CMG is enough.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Client Trusted Root Certificate to CMG | 1. Double-click on the certificate that was just created, issued and auto-enrolled and click the **Certification Path** tab. 2. Select the top-most certificate up the chain and click **View Certificate**. 3. On the new Certificate window, click the **Details** tab and click **Copy to File**. 4. In the Certificate Export Wizard, click **Next**. 5. On the Export File Format page, select **DER encoded binary X.509 (.CER)** and click **Next**. 6. On the File to Export page, **Browse** to a suitable location to save the certificate, specify the name of the **CER** file to be exported, and then click **Save | Next**. 7. To close the wizard, click **Finish** in the Certificate Export Wizard page, and then click **OK** in the confirmation dialog box. 8. Store the file securely. Client trusted root certificate to CMG is required when using client authentication certificate. Ensure that you can access it from the ConfigMgr console. This certificate will also be required during setting up CMG. Close all the windows. |

### Configure Azure Services

Perform the following steps to configure Azure services in ConfigMgr.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure Azure Services | 1. In the ConfigMgr console, navigate to **Administration | Cloud Services | Azure Services**. 2. Right-click **Azure Services** and click **Configure Azure Services**. 3. On the Azure Services page, specify a **Name**, an “optional” **Description**, select **Cloud Management** and click **Next**. 4. On the App page, ensure **AzurePublicCloud** is selected next to **Azure environment**. 5. Click **Browse** next to **Web app**. 6. On the Server App window, click **Create**. 7. On the Create Server Application window, provide a friendly name for the app next to **Application Name**. 8. For the **HomePage URL**, specify a URL. By default, this value is **https://ConfigMgrService**. 9. For the **App ID URI**, specify a unique URL. By default, this value is **https://ConfigMgrService**. 10. For the **Secret key validity period**, select either **1 Year** or **2 Years**. By default, this value is **1 Year**. 11. Click **Sign in** next to **Azure AD Admin Account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Azure AD Tenant Name** is displayed. 12. On the Create Server Application window, click **OK**. 13. On the Server App window, select/highlight the app and click **OK**. 14. Back on the App page, click **Browse** next to **Native Client app**. 15. On the Client App window, click **Create**. 16. On the Create Client Application window, provide a friendly name for the app next to **Application Name**. 17. Click **Sign in** next to **Azure AD Admin Account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Azure AD Tenant Name** is displayed. 18. On the Create Client Application window, click **OK**. 19. On the Client App window, select/highlight the app and click **OK**. 20. Back on the App page, click **Next**. 21. On the Discovery page, select the checkbox next to **Enable Azure Active Directory User Discovery** and **Enable Azure Active Directory Group Discovery**. Both of them are not requirements for CMG. 22. On the Discovery page, click **Next**. 23. On the Summary page, review and click **Next**. 24. On the Completion page, click **Close**. |

### Set up the CMG along with CDP

This section provides the steps required to set up a CMG.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Set up the CMG along with CDP | 1. In the ConfigMgr console, navigate to **Administration | Cloud Services | Cloud Management Gateway**. 2. Right-click **Cloud Management Gateway** and click **Create Cloud Management Gateway**. 3. On the General page, ensure **AzurePublicCloud** is selected next to **Azure environment**. 4. Click **Sign In** next to **Subscription admin account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Subscription ID**, **Azure AD app name** and **Azure AD tenant name** fields are auto-populated with the respective values. 5. On the General page, click **Next**. 6. On the Settings page, click **Browse** next to **Certificate file** and select the CMG server authentication certificate exported earlier. 7. On the Password window prompt, specify the password and click **OK**. The **Service name** and **Deployment name** fields are auto-populated with the respective values. 8. Select the appropriate **Region** from the drop-down list. 9. Next to **Resource Group**, select **Create new** and specify the name of the resource group. 10. Next to **VM Instance**, enter the number of VMs for CMG. The default value is **1**, but you can scale up to 16 VMs per CMG. 11. Click **Certificates** next to Certificates uploaded to the cloud service. 12. On the Certificates uploaded to the cloud service window, click **Add** and select the client trusted root certificate to CMG exported earlier and click **OK**. 13. By default, the wizard enables the option to **Verify Client Certificate Revocation**. A certificate revocation list (CRL) must be publicly published for this verification to work. If you do not publish a CRL, deselect this option. 14. At the bottom, notice the option **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. This option is enabled by default. Keep it selected. 15. On the Settings page, click **Next**. 16. On the Alerts page, to monitor CMG traffic with a 14-day threshold, select the checkbox next to **Turn on 14-day threshold and alerts for monitoring outbound data transfer** and **Stop this service when the critical threshold is exceeded**. Then, specify the **14-day threshold for outbound data transfer (GB)**, **Percentage of threshold for raising Warning alert** and **Percentage of threshold for raising Critical alert**. 17. Also, select the checkbox next to **Specify storage alert threshold** and then specify the **Storage alert threshold (GB)**, **Generate Warning alert (% of storage alert threshold)** and **Generate Critical alert (% of storage alert threshold)** and then click **Next**. 18. On the Summary page, review and click **Next**. 19. On the Completion page, click **Close**. 20. At this stage, ConfigMgr starts setting up the service. It will take between 5 to 15 minutes to provision the service completely in Azure. Check the **Status** column for CMG, to determine when the service is **Ready**. 21. The CDP will be visible from **Administration | Distribution Points**. |

### Configure Boundary Group and Distribution Point Group for CDP

This section provides the steps to add the CDP to the Boundary Group and the Distribution Point Group.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure Boundary Group and Distribution Point Group for CDP | 1. In the ConfigMgr Console, browse to **Administration | Overview | Hierarchy Configuration | Boundary Groups**. Right-click on **Corp Boundary Group** which has the **Default Boundary** and the **IP Based Boundary** as members and click **Properties**. 2. Click the **References** tab and click **Add** under Site system servers. 3. Select the CDP and click **OK** and then click **OK** again. 4. In the ConfigMgr Console, browse to **Administration | Overview | Distribution Point Groups**. Right-click on the **Corp DPs** distribution point group and click **Properties**. 5. Click the **Members** tab and click **Add**. 6. Select the CDP and click **OK** and then click **OK** again. |

### Configure Enhanced HTTP and the Primary Site for Client Certificate Authentication

This section provides the steps to configure Enhanced HTTP and the Primary Site for Client Certificate Authentication.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure Enhanced HTTP and the Primary Site for Client Certificate Authentication | 1. In the ConfigMgr Console, browse to **Administration | Overview | Site Configuration | Sites**. 2. Right-click the primary site and click **Properties**. 3. In the primary site properties window, click the **Communication Security** tab and select the checkboxes next to **Use Configuration Manager-generated certificates for HTTP site systems** and **Use PKI client certificate (client authentication capability) when available**. 4. If you do not publish a CRL, deselect the option for **Clients check the certificate revocation list (CRL) for site systems**. 5. Under **Trusted Root Certification Authorities**, click **Set** and then in the Set Root CA Certificates window, click the **star** button and select the client trusted root certificate to CMG exported earlier. Click **OK**. 6. Click **Apply** and **OK**. |

### Add the CMG Connection Point

The CMG connection point is the site system role for communicating with CMG. This section provides the steps required to add the CMG connection point on the ConfigMgr site server.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Add the CMG Connection Point | 1. In the ConfigMgr console, navigate to **Administration | Site Configuration | Servers and Site System Roles**. 2. Right-click the primary site server where CMG connection point needs to be added and click **Add Site System Roles**. 3. On the General page, click **Next**. 4. On the Proxy page, click **Next**. 5. On the System Role Selection page, select **Cloud management gateway connection point** and click **Next**. 6. On the Cloud management gateway connection point page, select the **Cloud management gateway name** to which the server connects to. The **Region** is auto-populated based on the selected Cloud management gateway name. Click **Next**. 7. On the Summary page, review and click **Next**. 8. On the Completion page, click **Close**. 9. After few minutes, you can check the status of the CMG connection point on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, the **Connection Status** of the **Connection Point Server Name** shows **Connected** under the **Connection Points** tab. |

### Configure the Management Point and Software Update Point for CMG Traffic

The management point and the software update point need to be configured to accept CMG traffic. This section provides the steps required to configure the management point and software update point for CMG traffic.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure the Management Point and Software Update Point for CMG Traffic | 1. In the ConfigMgr console, navigate to **Administration | Site Configuration**, right-click **Servers and Site System Roles** and select **Management point**. 2. Select the site server which needs to be configured for CMG traffic and right-click **Management point | Properties**. 3. In the **General** tab of the Management point Properties window, under **Client connections**, ensure that **HTTP** is selected. 4. Select the checkbox next to **Allow Configuration Manager cloud management gateway traffic**. 5. Ensure **Allow intranet and Internet connections** is selected automatically. 6. Click **Apply** and **OK**. 7. After few minutes, you can even check the status of the management point endpoints on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, under **Role Endpoints** tab, you are able to see management point endpoints. 8. Navigate to **Administration | Site Configuration**, right-click **Servers and Site System Roles** and select **Software update point**. 9. Select the site server which needs to be configured for CMG traffic and right-click **Software update point | Properties**. 10. In the Software update point Properties window, select the checkbox next to **Allow Configuration Manager cloud management gateway traffic**. 11. Ensure **Allow Internet and intranet client connections** is selected automatically. 12. Ensure that the checkbox next to **Require SSL communication to the WSUS server** is unchecked and click **Apply** and **OK**. 13. After few minutes, you can even check the status of the software update point endpoints on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, under **Role Endpoints** tab, you are able to see software update point endpoints. |

### Configure the Configuration Manager Client Settings for CMG and CDP

This section provides the steps required to configure the ConfigMgr Client Settings for CMG and CDP.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure the Configuration Manager Client Settings for CMG and CDP | 1. In the ConfigMgr Console, browse to **Administration | Overview | Client Settings** and double-click on **Default Client Settings**. 2. Click **Cloud Services** and then select **Yes** for **Allow access to cloud distribution point**. Also ensure that **Yes** is selected next to **Enable clients to use a cloud management gateway** and then click **OK**. 3. To verify, from **Assets and Compliance | Overview | Devices**, ensure that the ConfigMgr Client is installed on the clients and are active, example **CLIENT1**. From there, also ensure that the **Resultant Client Settings** show the changes made in the Default Client Settings. Right-click on the client, click **Client Settings | Resultant Client Settings**. |

### Test a Deployment on a Client on the Internet

In this section, you will create an application, distribute its contents to CDP and deploy the application to CLIENT1, which is simulated to be on the Internet.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 and CM1 virtual machine.** | |
| Test a Deployment on a Client on the Internet | 1. Before making any changes in **CLIENT1**, restart the **SMS Agent Host** service when it is on the Intranet. 2. Now, simulate **CLIENT1** to be on the Internet, by configuring the following registry key - **HKLM\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 1** and restart the **SMS Agent Host** service. 3. On **CLIENT1**, after few minutes, when you open the **ConfigMgr Client Properties**, under the **General** tab, notice that **Client certificate = PKI**, **Connection Type = Always Internet** and the **Network** tab shows the **FQDN of the CMG**. 4. In **CM1**, **download** a sample application, example **XML Notepad** and **create an application** in the ConfigMgr Console. After that **distribute** the application to **CDP** only and **deploy** it on **CLIENT1** as an **Available** deployment. Create a device collection for **CLIENT1**. 5. On **CLIENT1**, in the **ConfigMgr Client Properties**, **Actions** tab, run **Machine Policy Retrieval and Evaluation Cycle**. 6. On **CLIENT1**, when the notification appears that the software is available for the installation, open the **Software Center**, select the application and install it. The contents of the application will be downloaded from CDP to the ConfigMgr client cache and further installed from the ConfigMgr client cache.   **Note:** For further labs, change the value of the registry key created in **CLIENT1**, which simulated it being on the Internet - **HKLM\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 0** and then restart the **SMS Agent Host** service. |

## Tenant Attach, Co-Management and Switching Workloads

In Configuration Manager, co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Intune. It’s a solution that provides a bridge from on-premises to modern cloud management and gives you a path to make the transition using a phased approach.

After you enable co-management, Configuration Manager continues to manage all workloads. When you decide that you are ready, you can have Intune start managing available workloads. You can have Intune manage the following workloads: Compliance policies, Windows Update for Business policies, Resource Access policies, Endpoint Protection and many more.

For more information on Microsoft Endpoint Manager tenant attach: Device sync and device actions, refer to - <https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/device-sync-actions>

For more information on Troubleshooting device actions for Configuration Manager devices, refer to - <https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/technical-reference>

For more information on How to enable co-management in Configuration Manager, refer to - <https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-enable>

For more information on How to switch Configuration Manager workloads to Intune, refer to - <https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-switch-workloads>

### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Prerequisite Sections** | **Section 2.2 Cloud Environment**  **Section 3.3.4 Configure Azure AD Connect with Device Sync - All Steps**  **Section 5.2 Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP): All Sub-Sections - All Steps**  **Section 9.4 Windows AutoPilot**  **Section 9.4.1 Prerequisites – All Steps**  **Section 9.4.5 Configure AutoPilot – All Steps** |
| **Complete these steps on an Internet-connected Windows computer.** | |
| Enable Device Management. Set Mobile Device Management Authority (If MDM Authority is not equal to Intune) | **Note**: Before you can enroll mobile devices, you must prepare the Intune service by selecting the appropriate mobile device management authority setting on the Mobile Device Management page of the Administration workspace. The mobile device management authority setting determines whether you manage mobile devices with Intune or Configuration Manager with Intune integration. This guidance assumes Intune is used without Configuration Manager integration so the setting should be set to Microsoft Intune.   1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **All services > search for and click Intune > Intune**. 5. Select **Device enrollment**. 6. Under Mobile Device Management Authority, select **Intune MDM Authority** and click **Choose**. |
| Configure Auto MDM Enrollment for Intune | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune**. 5. In the **MDM user scope** setting, select **All**. 6. Click **Save**. |

### Tenant Attach, Co-Management and Switch Workloads

Once co-management is enabled, devices in the Pilot group can automatically enroll into Intune. This requires using a verified domain during the Setup Process of Azure AD Connect.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Device Collection | 1. Open the **Configuration Manager Console**, browse to **Assets and Compliance** workspace and select **Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. Input the following information:   *General*  Name – Enter **Co-managed Devices**  Limiting collection – Select **All Desktop and Server Clients** and click **Next**.  Select **Use incremental updates for this collection**.  Click **Next**.  Accept the Warning.   1. *Summary* – click **Next**, click **Close**. |
| Add a Device to the Collection | 1. In the **Assets & Compliance** workspace, select **Devices** and right-click **CLIENT1**. 2. Select **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 3. Select **Co-managed Devices** and click **OK**. 4. Select **Device Collections**, right-click **Co-managed Devices**, and select **Update Membership**. Click **Yes** on the warning box to continue. |
| Tenant Attach, Co-Management & Switch Workloads | 1. Open the **Configuration Manager Console**, browse to **Administration > Cloud Services > Co-management**. 2. Click **Configure co-management** from the ribbon bar. 3. In the **Co-management Configuration Wizard,** select **AzurePublicCloud** for your environment. 4. Sign in to Intune using **labadmin@<AzureDomainName>.onmicrosoft.com.** Click **Next** and accept the prompt. 5. On the **Configure upload** page, accept the defaults and click **Next**. 6. On the **Enablement** page, select **Pilot** next to **Automatic enrollment in Intune.** Click **Next.** 7. Under **Intune Auto Enrollment**., browseand select **Co-managed Devices.** Click **Next.** 8. On the **Workloads** page, drag the slider for **Compliance policies** and **Windows Update policies** to **Pilot Intune** and click **Next**. 9. On the **Staging** page, next to **Compliance Policies**, browse to **Co-managed Devices.** Scroll down and, next to **Windows Update Policies,** browse to **Co-managed Devices** and click **Next** to initiate configuration. 10. Click **Next** on the **Summary** page. Click **Close**. |
| Perform Device Actions | 1. In a browser, navigate to **endpoint.microsoft.com** and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 2. Select **Devices** then **All devices** to see the uploaded devices. You'll see **ConfigMgr** in the **Managed by** column for uploaded devices. 3. Select a device to load its **Overview** page. 4. Choose any of the following actions:    1. **Sync Machine Policy**    2. **Sync User Policy** 5. **App Evaluation Cycle** |
| Check device status | 1. Navigate to **endpoint.microsoft.com** and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 2. Select **Devices>Overview** see device status. 3. Click on **Devices>All devices. Click on a device labeled “Co-Managed” under the “ManagedDevices” column. These devices include telemetry generated through Tenant Attach (Intune + ConfigMgr-related items such as App Configurations).** 4. On left nav, click **Timeline**. Click **Filter** in top nav and change dates to expand time range by 7-10 days. Click **Apply** to see timeline of device events. Click on an event for details. (To add events, restart the device, add updates, etc.) |

### Co-Manage Devices with the Configuration Manager Client

For unverified domains, co-management can still be enabled by enrolling the domain-joined device into Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Log in to Client 1 | 1. Start/restart the VM and log in as **labadmin@<AzureDomainName>.onmicrosoft.com** with password **P@ssw0rd**. 2. Open the **Configuration Manager Client Applet** and under the **Actions** tab, run the **Machine Policy Retrieval & Evaluation Cycle** and then close the applet. Under **C:\Windows\CCM\Logs**, monitor the **CoManagementHandler.log**. At this stage, Co-management will get automatically enabled on the device and will also automatically enroll the device to Intune. 3. After a while, reopen the **Configuration Manager Client Applet** and under the **General** tab, notice the **Co-management capabilities=19** and **Co-management=Enabled**. 4. Under the **Configurations** tab, **Evaluate** and **Refresh** the following settings to make them **Compliant**:  * **CoMgmtSettingsPilotAutoEnroll** * **CoMgmtSettingsPilotCP** * **CoMgmtSettingsPilotWUP** * **CoMgmtSettingsProd** |
| **Complete these steps from an internet-connected Windows computer.** | |
| Check the Windows 10 Device | **Note**: In this example, we will look in Microsoft Intune to see the device details and we can see that it already recognizes Windows 10 as an operating system in Microsoft Intune.   1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Devices**. 4. Notice that the Windows 10 device (**CLIENT1**) is **Hybrid Azure AD joined**. 5. On the left navigation bar, click **All services > search for and click Intune > Intune**. 6. Select **Devices** > **All devices**. 7. Notice that the Windows 10 device (**CLIENT1**) is **Co-managed**. 8. Click on the Windows 10 device (**CLIENT1**). Notice the **device actions** like **Sync**. Also, notice the **Co-management** statement, **Configuration Manager agent state**, **Details**, **Last Configuration Manager agent check in time** and **Intune managed workloads**. Notice both the workloads - **Compliance Policy** and **Windows Update for Business**. |

### AutoPilot (Configuration Manager Client Installation from Cloud Management Gateway – CMG)

For devices provisioned using the AutoPilot service and for those devices to have the Configuration Manager Client installed from CMG, there are two things that need to be deployed from Intune:

* Client Trusted Root Certificate (Section 5.2.8)
* Configuration Manager Client

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Deploy the Client Trusted Root Certificate | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **All services > search for and click Intune > Intune**. 5. Select **Device configuration**. 6. Under **Manage**, select **Profiles**. 7. Click **+ Create profile**. 8. Under **Platform**, select **Windows 10 and later** and under **Profile**, select **Trusted certificate**. Click **Create**. 9. Under the **Basics** tab, enter the following and click **Next**:   **Name: Trusted Root Certificate**   1. Under the **Configuration settings** tab, enter the following and click **Next**:   Browse to **C:\Packages** and select the **Client Trusted Root Certificate** created in **Section 5.2.8**  **Destination store: Computer certificate store – Root**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**, select **AutoPilot Devices**, click **Select**.   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| Deploy the Configuration Manager Client | 1. Select **Client apps > Apps > + Add**. 2. Under **App type**, select **Line-of-business app** and click **Select**. 3. Under the **App information** tab, enter the following and click **Next**:   Click **Select app package file** and browse to **C:\Program Files\Microsoft Configuration Manager\bin\i386\ccmsetup.exe**. Click **OK**.  **Publisher: Microsoft**  **Command-line arguments: Enter the command line from the Configuration Manager Console > Administration > Cloud Services > Co-management > Right-click CoMgmtSettingsProd > Properties > Enablement tab > Copy the Command-line arguments from there**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Add group**, select **AutoPilot Devices**, click **Select**.   1. Under the **Review + create** tab, click **Create**. Once the upload is completed, wait for a few minutes for the page to refresh. |
| **Complete these steps from the CLIENT4 virtual machine.** | |
| Perform Azure AD Join | 1. Start the VM and once OOBE has started, in the **Hi Test User1! Welcome to Microsoft Services** pane, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**. 2. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 3. In the **All set!** pane, click **OK**. |
| Validate Azure AD Join and MDM Enrollment | 1. Go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Confirm that **Connected to <CompanyName>’s Azure AD** is displayed and the **Info** button is displayed as well. Notice the **ConfigMgr Client Setup Bootstrap: EnforcementCompleted message**. If required click **Sync**. After a while the Configuration Manager Client will be installed from the Cloud Management Gateway. |
| **Complete these steps from an internet-connected Windows computer.** | |
| Validate Azure AD and MDM Enrollment | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Devices**. 4. Notice that the Windows 10 device (**CLIENT1**) is **Azure AD joined**. 5. On the left navigation bar, click **All services > search for and click Intune > Intune**. 6. Select **Devices** > **All devices**. 7. Notice that the Windows 10 device (**CLIENT4**) is **Co-managed**. 8. Click on the Windows 10 device (**CLIENT1**). Notice the **device actions** like **Sync**. Also, notice the **Co-management** statement, **Configuration Manager agent state**, **Details** and **Last Configuration Manager agent check in time**. |
| **Complete these steps from the HYPER-V Host.** | |
| Revert Virtual Machines | 1. Revert **HYD-CLIENT4** to the latest checkpoint. |

## Endpoint Analytics

Endpoint analytics is part of the [Microsoft Productivity Score](https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/productivity-score). These analytics give you insights for measuring how your organization is working and the quality of the experience you're delivering to your users. **Endpoint analytics** aims to improve user productivity and reduce IT support costs by providing insights into the user experience. The insights enable IT to optimize the end-user experience with proactive support and to detect regressions to the user experience by assessing user impact of configuration changes.

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps in browser.** | |
| Onboard in the Endpoint analytics portal | 1. Go to https://aka.ms/endpointanalytics 2. Choose from the following options:    1. **All cloud-managed devices**: Creates an [Intune data collection policy](https://docs.microsoft.com/en-us/mem/analytics/settings#bkmk_profile) assigned to all Windows 10 1903 or later devices which are either Intune managed or co-managed.    2. **Selected devices**: Creates and assigns the policy to devices which you select.    3. **I'll choose later**: Doesn't deploy a policy to devices. Proactive remediations can still be used, but any reports that rely on analytics data will be empty. 3. Click **Start**. This will automatically assign a configuration profile to collect boot performance data from all eligible devices. You can [change assigned devices](https://docs.microsoft.com/en-us/mem/analytics/settings#bkmk_profile) later. It may take up to 24 hours for startup performance data to populate from your Intune enrolled devices after they reboot. |
| View the Overview page | Note: You won't see your data immediately. The data needs to be gathered and the results calculated. For startup performance, the device needs to have been restarted at least once. Once your data is ready, you'll notice some information on the **Overview** page, explained in more detail [here.](https://docs.microsoft.com/en-us/mem/analytics/enroll-intune)  Endpoint analytics overview page |

## Remote Access (VPN)

Virtual private networks (VPNs) give your users secure remote access to your company network. Devices use a VPN connection profile to initiate a connection with the VPN server. In this section, you will go through how to manage and deploy VPN on Windows 10.

### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the INET1 virtual machine.** | |
| Configure Internet DNS | 1. Click the **Start** button and browse to **Windows Administrative Tools > DNS**. 2. In the **DNS Manager** window, browse to **INET1 > Forward Lookup Zones > contoso.com**. 3. Right-click on **contoso.com** and select **New Host (A or AAAA)**. 4. In the **New Host** window, under **Name** enter **vpn1**, under **IP address** enter **131.107.0.2** then click **Add Host**. 5. Click **OK | Done**. |
| **Complete these steps on the DC1 virtual machine.** | |
| Add VPN1 Server to RAS and IAS Server AD Group | 1. Click the **Start** button and browse to **Windows Administrative Tools > Active Directory Users and Computers**. 2. Browse to **corp.contoso.com > Users**. 3. Right-click on the **RAS and IAS Servers** group and select **Properties**. 4. Go to the **Members** tab and ensure that **VPN1** is present. 5. In the **RAS and IAS Servers Properties** window, click **OK**. |
| Create VPN Certificate Template | 1. Click the **Start** button and browse to **Windows Administrative Tools > Certification Authority**. 2. Browse to **corp-DC1-CA > Certificate Templates**. 3. Right-click on **Certificate Templates** and select **Manage**. 4. Right-click on the **IPSec** template and select **Duplicate Template**. 5. In the **Properties of New Template** window, go to the **General** tab. 6. Under **Template display name**, enter **VPN Server** then go to the **Request Handling tab**. 7. Select **Allow private key to be exported** then go to the **Subject Name** tab. 8. Select **Supply in the request**, click **OK** in the dialog box then go to the **Extensions** tab. 9. Under **Extensions included in this template**, select **Application Policies** then click **Edit**. 10. In the **Edit Application Policies Extension** window, click **Add**. 11. In the **Add Application Policy** window, select **Server Authentication** then click **OK**. 12. In the **Edit Application Policies Extension** window, click **OK**. 13. In the **Properties of New Template** window, click **Apply | OK**. 14. **Close** the **Certificate Templates Console** and go back to the **Certification Authority** MMC. 15. Right-click on **Certificate Templates** and select **New > Certificate Template to Issue**. 16. In the **Enable Certificate Templates** window, select **VPN Server** then click **OK**. |
| Create Workstation Certificate Template | 1. Click the **Start** button and browse to **Windows Administrative Tools > Certification Authority**. 2. Browse to **corp-DC1-CA > Certificate Templates**. 3. Right-click on **Certificate Templates** and select **Manage**. 4. Right-click on the **Workstation Authentication** template and select **Duplicate Template**. 5. In the **Properties of New Template** window, go to the **General** tab. 6. Under **Template display name**, enter **Contoso PC** then go to the **Request Handling tab**. 7. Select **Allow private key to be exported** then, go to the **Subject Name** tab. 8. Under **Subject name format,** select **Common name** then, go to the **Security** tab. 9. Select **Domain Computers (CORP\Domain Computers)** and select **Read** and **Autoenroll**. Click **Apply | OK**. 10. **Close** the **Certificate Templates Console** and go back to the **Certification Authority** MMC. 11. Right-click on **Certificate Templates** and select **New > Certificate Template to Issue**. 12. In the **Enable Certificate Templates** window, select **Contoso PC** then click **OK**. 13. Click the **Start** button and browse to **Windows Administrative Tools > Group Policy Management**. 14. Expand **Forest: corp.contoso.com | Domains | corp.contoso.com**. 15. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here**. 16. Under **Name**, type **Client Authentication Certificate Autoenrollment VPN** and click **OK**. 17. Right-click **Client Authentication Certificate Autoenrollment VPN** and click **Edit**. 18. Browse to **Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies**. 19. Double-click **Certificate Services Client – Auto-Enrollment**. Select **Enabled** for **Configuration Model** and check the boxes next to **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**. Click **Apply | OK**. |
| Create User Certificate Template | 1. Click the **Start** button and browse to **Windows Administrative Tools > Certification Authority**. 2. Browse to **corp-DC1-CA > Certificate Templates**. 3. Right-click on **Certificate Templates** and select **Manage**. 4. Right-click on the **User** template and select **Duplicate Template**. 5. In the **Properties of New Template** window, go to the **General** tab. 6. Under **Template display name**, enter **Contoso User** then go to the **Request Handling tab**. 7. Select **Allow private key to be exported** then, go to the **Subject Name** tab. 8. Under **Build from this Active Directory information,** configure the following then click **Apply | OK**.   **Subject name format**: Fully distinguished name  **Include e-mail name in subject name**: Deselect  **E-mail name**: Deselect  **User principal name (UPN)**: Selected   1. **Close** the **Certificate Templates Console** and go back to the **Certification Authority** MMC. 2. Right-click on **Certificate Templates** and select **New > Certificate Template to Issue**. 3. In the **Enable Certificate Templates** window, select **Contoso User** then click **OK**. |
| **Complete these steps on the VPN1 virtual machine.** | |
| Request VPN Certificate | 1. Reboot **VPN1** once. 2. Right-click on the **Start** button and select **Run**. 3. In the **Run** window, enter **certlm.msc** then click **OK**. Accept the UAC prompt. 4. Right-click on **Personal** and select **All Tasks > Request New Certificate**. 5. In the **Before You Begin** page, click **Next**. 6. In the **Select Certificate Enrollment** **Policy** page, click **Next**. 7. In the **Request Certificates** page, select **VPN Server** then click **More information is required to enroll for this certificate. Click here to configure settings**. 8. Under **Subject name**, select the **Type** as **Common name**, under **Value** enter **VPN1.corp.contoso.com** then click **Add**. 9. Under **Alternative name**, select the **Type** as **DNS**, under **Value** enter **VPN1.contoso.com** then click **Add**. 10. In the **Certificate Properties** window, click **Apply | OK**. 11. In the **Request Certificates** page, click **Enroll**. 12. In the **Certificate Installation Results** page, click **Finish**. |
| Configure IKEv2 Machine Authentication | 1. Click the **Start** button and browse to **Windows Administrative Tools > Routing and Remote Access**. 2. Right-click on **VPN1** then select **Properties**. 3. In the **VPN1 (local) Properties** window, go to the **Security** tab. 4. Click **Authentication Methods**. 5. In the **Authentication Methods** window, ensure that **Allow machine certificate authentication for IKEv2** is selected, then click **OK**. 6. In the **VPN1 (local) Properties** window, click **Cancel**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Request Client Certificates | 1. Reboot **CLIENT2** once. 2. Right-click on the **Start** button and select **Run**. 3. In the **Run** window, enter **mmc** then click **OK**. Accept the UAC prompt if required. 4. In the **MMC** window, click **File > Add/Remove Snap-in**. 5. In the **Add or Remove Snap-ins** window, select **Certificates** and click **Add**. 6. In the **Certificates snap-in** window, select **Computer** **account** then click **Next**. 7. In the **Select Computer** window, click **Finish**. 8. In the **Add or Remove Snap-ins** window, click **OK**. 9. Expand **Certificates (Local Computer) | Personal | Certificates**. You should be able to see the certificate. |
| Request User Certificates | 1. In the **MMC** window, click **File > Add/Remove Snap-in**. 2. In the **Add or Remove Snap-ins** window, select **Certificates** and click **Add**. 3. In the **Certificates snap-in** window, select **My user** **account** then click **Finish**. 4. In the **Add or Remove Snap-ins** window, click **OK**. 5. At the bottom, under **Certificates (Current User)**, right-click on **Personal** and select **All Tasks > Request New Certificate**. 6. In the **Before You Begin** page, click **Next**. 7. In the **Select Certificate Enrollment** **Policy** page, click **Next**. 8. In the **Request Certificates** page, select **Contoso** **User** then click **Enroll**. 9. Once complete, click **Finish**. |
| Copy VPN Scripts | 1. Right-click on the **Start** button and select **Run**. 2. In the **Run** window, enter **\\VPN1\c$** then click **OK**. 3. Open the **packages** folder. 4. **Copy** the **Scripts** folder to the root **C:** drive. |

### Manually Create VPN Profile

In this activity, you will configure VPN profiles manually on Windows 10.

#### Settings App

In this activity, you will configure VPN profiles through the Settings app.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Create VPN Profile | 1. Click on the **Start** button and select **Settings** (gear icon). 2. In the **Settings** app, browse to **Network & Internet > VPN**. 3. Click **Add a VPN connection**. 4. In the **Add a VPN connection** pane, configure the following and click **Save**.   VPN provider: **Windows (built-in)**  Connection name: **ContosoVPN**  Server name or address: **vpn1.contoso.com**  VPN type: **IKEv2**  Type of sign-in info: **Certificate**   1. Right-click on the **Start** button and select **Run**. In the **Run** window, enter **ncpa.cpl** then click **OK**. 2. In the **Network Connections** window, right-click on **ContosoVPN** and select **Properties**. 3. In the **ContosoVPN Properties** window, go to the **Security** tab. 4. Under **Authentication**, select **Use machine certificates** then click **OK**. |
| Connect to VPN | 1. In the **CLIENT2** Virtual Machine **Settings**, change the network from **Corpnet vSwitch** to **Internet vSwitch**. 2. In the **Settings** app, select **ContosoVPN** then click **Connect**. 3. Open a **command prompt** and **ping DC1.corp.contoso.com**.   **Note**: Ping should get a reply to confirm VPN connection. |
| Delete VPN Profile | 1. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 2. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

#### PowerShell and ProfileXML

In this activity, you will configure VPN profiles through PowerShell and ProfileXML.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Create VPN Profile | 1. Click the **Start** button and type **PowerShell**. Right-click **Windows PowerShell ISE** and select **Run as administrator**. 2. In the **User Account Control** window, click **Yes** if required. 3. In the **Windows PowerShell ISE** window, click **File > Open** and browse to **C:\Scripts** folder. 4. Select the **VPN\_Base.ps1** file and click **Open**. 5. Review elements in the script. 6. In the **PowerShell Console** pane, execute the following command:   ***Set-ExecutionPolicy -ExecutionPolicy Unrestricted***   1. Select **Yes to All**. 2. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. |
| Connect to VPN | 1. In the **Settings** app, select **ContosoVPN** then click **Connect**. 2. Open a **command prompt** and **ping DC1.corp.contoso.com**.   **Note**: Ping should get a reply to confirm VPN connection. |
| Delete VPN Profile | 1. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 2. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

### Configure Always-On

In this activity, you will configure VPN to be Always-On.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Always-On | 1. In the **Windows PowerShell ISE** for **VPN\_Base.ps1**, modify the script by adding the tag below after the **<DnsSuffix>** tag.   **<AlwaysOn>true</AlwaysOn>**   1. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. 2. Click **OK** in the dialog box. |
| Verify Always-On Configuration | 1. **Get-WmiInstance** output is displayed in the **PowerShell Console** pane. Scroll up the screen and review the **AlwaysOn** property to make sure it is set to **true**. |
| Test the Auto-Connection during a Network Change Event | 1. Open a **command prompt** and **ping DC1.corp.contoso.com –t**. 2. In the CLIENT2 Virtual Machine **Settings**, change the network from **Internet vSwitch** to **Corpnet vSwitch**.   **Note**: Wait for a couple of seconds to 1 minute before proceeding to the next step.   1. In the CLIENT2 Virtual Machine **Settings**, change the network from **Corpnet vSwitch** to **Internet vSwitch**. 2. View the **command prompt** and confirm VPN connection.   **Note**: Ping should get a reply to confirm VPN connection.   1. In the **Settings** app, confirm that **ContosoVPN** is **Connected**. |
| Test the Auto-Connection during a User Logon | 1. Close all applications and **sign-out**. 2. **Sign back in** and then open a **command prompt** and **ping DC1.corp.contoso.com**.   **Note**: Ping should get a reply to confirm VPN connection.   1. In the **Settings** app, confirm that **ContosoVPN** is **Connected**. |
| Delete VPN Profile | 1. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 2. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove.** In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

### Configure Trusted Network Detection

In this activity, you will walkthrough how to configure trusted network detection for VPN.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Trusted Network Detection | 1. Click the **Start** button and type **PowerShell**. Right-click **Windows PowerShell ISE** and select **Run as administrator**. 2. In the **User Account Control** window, click **Yes** if required. 3. In the **Windows PowerShell ISE** window, click **File > Open** and browse to **C:\Scripts** folder. 4. Select the **VPN\_Base.ps1** file and click **Open**. 5. In the **Windows PowerShell ISE** for **VPN\_Base.ps1**, modify the script by adding the tag below after the **<AlwaysOn>** tag.   **<TrustedNetworkDetection>contoso.com</TrustedNetworkDetection>**   1. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. 2. Click **OK** in the dialog box. |
| Verify Trusted Network Detection Configuration | 1. **Get-WmiInstance** output is displayed in the **PowerShell Console** pane. Scroll up the screen and review the **TrustedNetworkDetection** property to make sure it is set to **contoso.com**. |
| Test the Trusted Network Detection Configuration | 1. Open the **Settings** app and browse to **Network & Internet > VPN**. 2. In the **CLIENT2** Virtual Machine **Settings**, change the network from **Internet vSwitch** to **Not connected**. 3. In the **CLIENT2** Virtual Machine **Settings**, change the network from **Not connected** to **Internet vSwitch**.   **Note**: Wait for a couple of seconds to 1 minute before proceeding to the next step.   1. In the **Settings** app, confirm that **ContosoVPN** is **Connected** as expected. 2. In the **CLIENT2** Virtual Machine **Settings**, change the network from **Internet vSwitch** to **Corpnet vSwitch**. 3. In the **Settings** app, confirm that **ContosoVPN** is **Connecting** or **Not Connected**. |
| Delete VPN Profile | 1. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

### Configure App-Triggers

In this activity, you will walk through how to configure VPN application triggers.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Application Trigger | 1. Click the **Start** button and type **PowerShell**. Right-click **Windows PowerShell ISE** and select **Run as administrator**. 2. In the **User Account Control** window, click **Yes** if required. 3. In the **Windows PowerShell ISE** window, click **File > Open** and browse to **C:\Scripts** folder. 4. Select the **VPN\_Base2.ps1** file and click **Open**. 5. In the **Windows PowerShell ISE** for **VPN\_Base2.ps1**, modify the script by adding the tags below after the **</NativeProfile>** tag.   **<AppTrigger>**  **<App>**  **<Id>C:\Windows\System32\mstsc.exe</Id>**  **</App>**  **</AppTrigger>**   1. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. 2. Click **OK** in the dialog box. |
| Test the Application Trigger Configuration | 1. In the **CLIENT2** Virtual Machine **Settings**, change the network from **Corpnet vSwitch** to **Internet vSwitch**.   **Note**: Wait for a couple of seconds to 1 minute before proceeding to the next step.   1. In the **Settings** app, confirm that **ContosoVPN** is **Not** **Connected**.   **Note**: AlwaysOn tag was removed therefore the ContosoVPN profile did not automatically connect.   1. Right-click on the **Start** button and select **Run**. 2. In the **Run** window, enter **mstsc** then click **OK**. 3. In the **Remote Desktop Connection** window, connect to the **DC1.corp.contoso.com** server. 4. In the **Enter your credentials** window, log in as **corp\LabAdmin**. 5. In the **Settings** app, confirm that **ContosoVPN** is **Connected**.   **Note**: Launching the Remote Desktop application will trigger the ContosoVPN connection and will remain connected while the application is running. |
| Test Traffic across the VPN Connection | 1. Right-click on the **Start** button and select **Run**. 2. In the **Run** window, enter **\\DC1** then click **OK**.   **Note**: You will be able to connect to DC1 via SMB through the VPN connection. The VPN connection is not limited to RDP traffic.   1. **Close** the **SMB** and **RDC** connection to **DC1**. |
| Delete VPN Profile | 1. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 2. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

### Add Traffic Filters

In this activity, you will walk through how to configure VPN traffic filters.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Traffic Filters | 1. Click the **Start** button and type **PowerShell**. Right-click **Windows PowerShell ISE** and select **Run as administrator**. 2. In the **User Account Control** window, click **Yes** if required. 3. In the **Windows PowerShell ISE** window, click **File > Open** and browse to **C:\Scripts** folder. 4. Select the **VPN\_Base2.ps1** file and click **Open**. 5. In the **Windows PowerShell ISE** for **VPN\_Base2.ps1**, modify the script by adding the tags below after the **</AppTrigger>** tag.   **<TrafficFilter>**  **<App>**  **<Id>C:\Windows\System32\mstsc.exe</Id>**  **</App>**  **</TrafficFilter>**   1. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. 2. Click **OK** in the dialog box. |
| Test the Traffic Filter Configuration | **Note**: Make sure the VM is connected to the **Internet vSwitch**.   1. In the **Settings** app, confirm that **ContosoVPN** is **Not** **Connected**.   **Note**: AlwaysOn tag was removed therefore the ContosoVPN profile did not automatically connect.   1. Right-click on the **Start** button and select **Run**. 2. In the **Run** window, enter **mstsc** then click **OK**. 3. In the **Remote Desktop Connection** window, connect to the **DC1.corp.contoso.com** server. 4. In the **Enter your credentials** window, log in as **corp\LabAdmin**. 5. In the **Settings** app, confirm that **ContosoVPN** is **Connected**.   **Note**: Launching the Remote Desktop application will trigger the ContosoVPN connection and will remain connected while the application is running.   1. Right-click on the **Start** button and select **Run**. 2. In the **Run** window, enter **\\DC1** then click **OK**.   **Note**: You will not be able to connect to DC1 via SMB through the VPN connection. Only RDP traffic is allowed through the VPN connection. |
| Delete VPN Profile | 1. **Close** the **RDC** connection to **DC1**. 2. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 3. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**). |

### Configure Name-Based Connection Triggers

In this activity, you will walk through how to configure name based connection triggers for VPN.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Name-Based Connection Trigger | 1. Click the **Start** button and type **PowerShell**. Right-click **Windows PowerShell ISE** and select **Run as administrator**. 2. In the **User Account Control** window, click **Yes** if required. 3. In the **Windows PowerShell ISE** window, click **File > Open** and browse to **C:\Scripts** folder. 4. Select the **VPN\_Base3.ps1** file and click **Open**. 5. In the **Windows PowerShell ISE** for **VPN\_Base3.ps1**, modify the script by adding the tags below after the **</NativeProfile>** tag.   **<DomainNameInformation>**  **<DomainName>.</DomainName>**  **</DomainNameInformation>**  **<DomainNameInformation>**  **<DomainName>.corp.contoso.com</DomainName>**  **<DnsServers>10.0.0.6</DnsServers>**  **<AutoTrigger>true</AutoTrigger>**  **</DomainNameInformation>**   1. In the **Windows PowerShell ISE**, select the **Play** icon (Run Script) to execute the script. 2. Click **OK** in the dialog box. |
| Test the Name-Based Trigger Configuration | **Note**: Make sure the VM is connected to the **Internet vSwitch**.   1. In the **Settings** app, confirm that **ContosoVPN** is **Not** **Connected**.   **Note**: AlwaysOn tag was removed therefore the ContosoVPN profile did not automatically connect.   1. Open the **Microsoft Edge** browser from the taskbar. 2. In the **Microsoft Edge** window **address** bar, enter **http://DC1.corp.contoso.com**   **Note:** You might have to install **IIS** in **DC1** if it is not already installed.   1. In the **Settings** app, confirm that **ContosoVPN** is **Connected**.   **Note**: The IIS default page for DC1 will load. The ContosoVPN connection was initiated because there was a DNS query for \*.corp.contoso.com. |
| Delete VPN Profile | 1. **Close the Microsoft Edge browser.** 2. In the **Settings** app, select **ContosoVPN** then click **Disconnect**. 3. In the **Settings** app, select **ContosoVPN**, then click **Remove | Remove**. In case you are unable to delete the VPN Profile from the **Settings** app, you can delete it from the **Network Connections** window as well (**ncpa.cpl**).   **Note:** Ensure before proceeding with any other labs, that the VM’s virtual switch configuration is reverted to the configuration like it was before starting this lab, so that is connected to the **Corpnet vSwitch** and **External 2 vSwitch**. |

# Prepare Configuration

## Optimize Windows 10 Update Delivery

When considering your content distribution strategy for Windows 10, think about enabling a form of peer-to-peer content sharing to reduce bandwidth issues during updates. Windows 10 offers two peer-to-peer options for update content distribution: Delivery Optimization and BranchCache. These technologies can be used with several of the servicing tools for Windows 10. Two methods of peer-to-peer content distribution are available in Windows 10.

* [Delivery Optimization](https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization) is a new peer-to-peer distribution method in Windows 10. Windows 10 clients can source content from other devices on their local network that have already downloaded the updates or from peers over the internet. Using the settings available for Delivery Optimization, clients can be configured into groups, allowing organizations to identify devices that are possibly the best candidates to fulfil peer-to-peer requests. Windows Update, Windows Update for Business, and Windows Server Update Services (WSUS) can use Delivery Optimization. Delivery Optimization can significantly reduce the amount of network traffic to external Windows Update sources as well as the time it takes for clients to retrieve the updates.
* [BranchCache](https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache) is a bandwidth optimization technology that is included in some editions of Windows Server 2016 and Windows 10 operating systems, as well as in some editions of Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, and Windows 7.
* **Note:** Configuration Manager has an additional feature called Client Peer Cache that allows peer-to-peer content sharing between clients you use Configuration Manager to manage, in the same Configuration Manager boundary Group. For more information, see [Client Peer Cache.](https://docs.microsoft.com/sccm/core/plan-design/hierarchy/client-peer-cache)

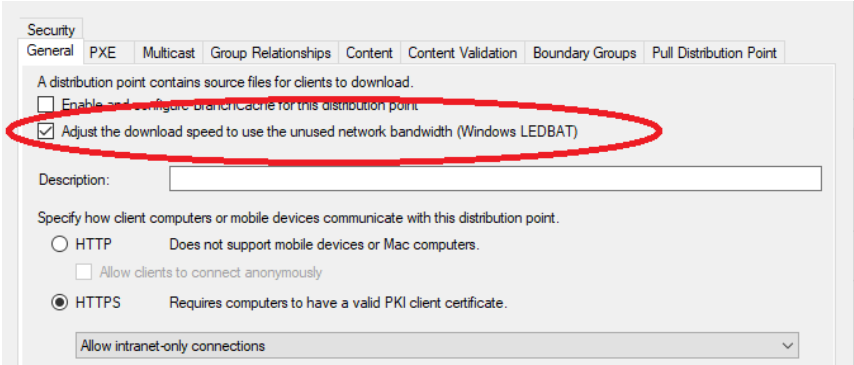
| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the DC1 virtual machine.** | | | |
| Configure Delivery Optimization | | 1. Go to **Server Manager>Tools>Active Directory Users and Computers** and right-click **CORP**, then click **New>Organizational Unit**. 2. Create an Organizational Unit, example “**Known Folder**” under **CORP** and add/move the **CLIENT7** and **CLIENT2** to this OU. 3. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 4. Right-click the Organizational Unit created “**Known Folder**” and click **Create a GPO in this domain, and Link it here**. Give it a name, example “ **Delivery Optimization**” and click **OK**. 5. Right-click the new GPO, example “**Delivery Optimization**” and click **Edit**. 6. Go to **Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization** to configureDelivery Optimization settings. 7. For info, see [**Configure Delivery Optimization for Windows 10 updates**](https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization). | |
| Enable Branch Cache on Client Computers | 1. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 2. Right-click the Organizational Unit created “**Known Folder**” and click **Create a GPO in this domain, and Link it here**. Give it a name, example “**Branch Cache**” and click **OK**. 3. Right-click the new GPO, example “**Branch Cache**” and click **Edit**. 4. Go to **Computer Configuration\Policies\Administrative Templates\Network**\**BranchCache to configure BranchCache settings.** 5. For info, see [**Branch Cache Client Configuration**](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/dd637820(v=ws.10)). | |

### Latency Optimized Background Transport (LEDBAT)

Keeping a network secure is a never-ending job for IT Pros, and doing so requires regularly updating systems to protect against the latest threat vectors. This is one of the most common tasks that an IT Pro must perform. Unfortunately, it can result in dissatisfaction for end-users as the network bandwidth used for the update can compete with interactive tasks that the end-user requires to be productive.

With **Windows Server 2019**, we bring a latency optimized, network congestion control provider called LEDBAT, which stands for Low Extra Delay Background Transfer. LEDBAT is designed to automatically yield bandwidth to users and applications, while consuming the entire bandwidth available when the network is not in use. It’s a scavenger protocol – it scavenges whatever network bandwidth is available on the network, and uses it. In other words, you can transfer Configuration Manager Packages or Microsoft Updates without interfering with your user’s sanity.

LEDBAT can also be enabled on a Configuration Manager distribution point running Windows Server 2019. Because LEDBAT operates on the sending side, any client **regardless of the operating system**, will enjoy the benefits that it brings. To enable this in Configuration Manager, check the following option:

[](https://msdnshared.blob.core.windows.net/media/2018/07/SCCM-LEDBAT.png)

For more information see:

* [Top 10 Networking Features in Windows Server 2019: #9 LEDBAT – Latency Optimized Background Transport](https://blogs.technet.microsoft.com/networking/2018/07/25/ledbat/)
* [Enable distribution points to use network congestion control](https://docs.microsoft.com/en-us/sccm/core/get-started/capabilities-in-technical-preview-1805#enable-distribution-points-to-use-network-congestion-control)

## Servicing Windows 10 using Group Policy

In this activity, you will configure Windows Update for Business deferral policies using Group Policy. Before configuring the Windows Update for Business Group Policy settings, consider a [deployment strategy](https://docs.microsoft.com/en-us/windows/deployment/update/waas-servicing-strategy-windows-10-updates) for updates and feature updates in your environment. For more guidance, see [Walkthrough: use Group Policy to configure Windows Update for Business.](https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-group-policy)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure a Deployment Ring | 1. Under **Server Manager**, open **Tools>Group Policy Management**. 2. Expand **Forest: corp.contoso.com > Domains > corp.contoso.com**. 3. Right-click **corp.contoso.com** and select **Create a GPO in this domain, and Link it here**. 4. In the **New GPO** dialog box, type **Windows Update for Business – Group 1** for the name of the new GPO and click **OK**. 5. Right-click the **Windows Update for Business – Group 1** GPO, and then click **Edit.** 6. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Update > Windows Update for Business**. 7. Right-click **Select when Preview Builds and Feature Updates are received**, and then click **Edit**. 8. In the **Select when Preview Builds and Feature Updates are received** Group Policy setting configuration, **Enable** the policy, and then configure the options – **Select the Windows readiness level for the updates you want to receive**, **After a Preview Build or Feature Update is released, defer receiving it for this many days** and **Pause Preview Builds or Feature Updates starting**. Click **Apply** and **OK**. 9. Right-click **Select when Quality Updates are received**, and then click **Edit**. 10. In the **Select when Quality Updates are received** Group Policy setting configuration, **Enable** the policy, and then configure the options – **After a quality update is released, defer receiving it for this many days** and **Pause Quality Updates starting**. Click **Apply** and **OK**. |

## Servicing Windows 10 using Microsoft Intune

### Device Management for Windows 10 using Microsoft Intune

In this lab, you will set up and configure Windows 10 Mobile Device Management (MDM) with Microsoft Intune.

#### Enable Base Device Management for Intune Standalone

After you complete the following tasks, you are ready to manage mobile devices and computers.

| Task | | Detailed Steps | |
| --- | --- | --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | | |
| Enable Device Management. Set Mobile Device Management Authority (If MDM Authority is not equal to Intune) | **Note**: Before you can enroll mobile devices, you must prepare the Intune service by selecting the appropriate mobile device management authority setting on the Mobile Device Management page of the Administration workspace. The mobile device management authority setting determines whether you manage mobile devices with Intune or Configuration Manager with Intune integration. This guidance assumes Intune is used without Configuration Manager integration so the setting should be set to Microsoft Intune.   1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Select **Device enrollment**. 6. Under Mobile Device Management Authority, select **Intune MDM Authority** and click **Choose**. | |
| Create Groups (If not present) | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 5. Click **+ New group**. 6. In the Group pane fill in the following values:   Group Type: **Microsoft 365**  Group Name: **Sales**  Membership Type: **Assigned**  Members: **Test User1** and **Test User2**   1. Click **Create**. | |
| Customize the Company Portal (If not already configured) | 1. On the left navigation bar, click **All services > search and click Intune > Intune**. 2. Select **Client apps** > **Customization** and click **Edit**. 3. Under the **Settings** tab, customize the page as per your convenience. 4. Click **Review + save** and then click **Save**. | |
| Verify the Company Portal Configuration (If not already verified) | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.manage.microsoft.com> and Sign in with **TU1@<AzureDomainName>.onmicrosoft.com**. 4. Review the company portal, browse to **Helpdesk** from the top left-hand corner and confirm that the customizations have been applied. | |

#### Enroll a Windows 10 Device

This section outlines how to enroll a Windows 10 device into Microsoft Intune for MDM.

**Note:** If **CLIENT3** has already been enrolled into Intune via Azure AD Join from the previous labs, disconnect it from Azure AD and cleanup the **CLIENT3** computer object from Azure AD and Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Enroll a Windows 10 Device in Intune | 1. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Click **Enroll only in device management**. 4. The **Setup a work or school account** dialog box will show, asking for your account to enroll the device. 5. Provide the **TU1@<AzureDomainName>.onmicrosoft.com** account and click **Next**. 6. In the **Microsoft Intune Enrollment** page, enter the **password** then click **Sign in**. Click **Got it**. 7. In the **Settings** app, you should see that the device is now connected to the corporate MDM. 8. Select **Connected to <CompanyName> MDM** then click **Info**. 9. Click **Sync** and confirm that the sync was **successful**. |
| **Complete these steps from an internet-connected Windows computer.** | |
| Check Windows 10 Device Enrollment in Microsoft Intune | **Note**: In this example, we will look in Microsoft Intune to see the device details and we can see that it already recognizes Windows 10 as an operating system in Microsoft Intune.   1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **All services > search and click Intune > Intune**. 4. Select **Devices** > **All devices**. 5. Click on the Windows 10 device that you have enrolled (**CLIENT3**). Observe the information that has been collected about the device in all the tabs. |

#### Configure Software Updates

In this activity, you will configure and manage **Windows 10 Update Rings** in Intune to form deployment rings and ensure that Windows 10 systems are kept up to date when new builds are released. An update ring includes a group of settings that configures when and how Windows 10 updates get installed. For more details see [Manage software updates in Intune.](https://docs.microsoft.com/en-us/intune/windows-update-for-business-configure)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Ring Policy | 1. In Intune, navigate to **Software updates > Windows 10 update rings**. Click “**+ Create profile**” to create an Update Ring policy. 2. In the **Basics** tab, enter a **Name**, a **Description** (optional), and then click **Next**. 3. In the **Update ring settings** tab, enter the following information and then click **Next**:    * **Servicing channel**: Set the channel from which the device receives Windows updates.    * **Microsoft product updates**: Choose to scan for app updates from Microsoft Update.    * **Windows drivers**: Choose to include or exclude Windows Update drivers during updates.    * **Quality update deferral period (days)**: Enter the number of days for which quality updates are deferred. You can defer receiving these Quality Updates up to 30 days from their release.    * **Feature update deferral period (days)**: Enter the number of days for which Feature Updates are deferred. You can defer receiving Feature Updates up to 365 days from their release.    * **Set feature update uninstall period (2 – 60 days): Enter the number of days within which Feature Updates can be uninstalled.**    * **Automatic update behavior with Active hours start and Active hours end**: Choose how automatic updates are installed, when to restart or reboot. For details, see [Update/AllowAutoUpdate](https://docs.microsoft.com/windows/client-management/mdm/policy-configuration-service-provider#update-allowautoupdate).    * **Restart checks**: Enabled by default. When you restart a device, there are some checks that occur, including checking for active users, battery levels, running games, and more. To skip these checks when you restart a device, select **Skip.**    * **Option to pause Windows updates**    * **Option to check for Windows updates**    * **Require user approval to dismiss restart notification**    * **Remind user prior to required auto-restart with dismissible reminder (hours)**    * **Remind user prior to required auto-restart with permanent reminder (minutes)**    * **Change notification update level**    * **Use deadline settings** with **Deadline for feature updates**, **Deadline for quality updates**, **Grace period** and **Auto reboot before deadline** |
| Assign Ring | 1. In the **Assignments** tab, choose **+** **Select groups to include**, and then choose a group. 2. When finished, choose **Select | Next** to complete the assignment. 3. In the **Review + create** tab, click **Create**. |
| View Update Compliance | 1. Select **Software updates** > **Overview**. You can see information about the status of any update rings you assigned to devices and users.    * + Select **Software updates > Windows 10 update rings > Select the deployment ring > Overview**. You can see information about the status of the specific deployment ring you assigned to devices and users. |
| Pause Updates | 1. Select **Software updates** > **Windows 10 update rings > Select the deployment ring > Overview**. 2. Choose **Pause**. |
| Uninstall the Latest Software Updates | 1. In Intune, select **Software updates**. 2. Select **Windows 10 update rings > Select the deployment ring > Overview > Uninstall**. |

#### Configure Policy Settings and Policies based on OMA-URI

This section outlines how to configure Policies for Windows 10 in Intune available through the Intune Interface and a Policy through OMA-URI.

Use the Microsoft Intune Windows Phone OMA-URI Policy to deploy OMA-URI (Open Mobile Alliance Uniform Resource Identifier) settings that can be used to control features on Windows Phone Devices. These are standard settings that many mobile device manufacturers use to control device features.

This capability is intended to allow you to deploy Windows 10 Settings that are not configurable with an Intune Policy. For information about the Settings you can configure with these Policies, see Configure Security Policy for Mobile Devices in Microsoft Intune.

For help creating OMA-URI Settings for Windows 10 Services, see Windows Phone 10 CSP Documentation - <http://aka.ms/win10csp>.

**Note:** If any of the below policies conflicts with the policies from the previous labs, delete the policies from the previous labs.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create an OMA-URI Policy to Disable Cortana | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **All services > search and click Intune > Intune**. 4. Select **Device configuration** > **Profiles** > **+** **Create profile**. 5. Under **Platform**, select **Windows 10 and later**. 6. Under **Profile type**, select **Custom** and click **Create**. 7. Under the **Basics** tab, enter the following information and click **Next**:   In the **Name** field, type **Windows 10 – Disable Cortana**.   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Click **Add**.  In the **Name** field enter **Windows 10 – Disable Cortana**.  In the **OMA-URI** field enter (Case sensitive and starting with a period):  **./Vendor/MSFT/Policy/Config/Experience/AllowCortana**  For **Data type** select **Integer**.  For **Value** enter **0** (0 means the setting is not allowed).  Click **Add**.   1. Under the **Assignments** tab, enter the following information and click **Next**:   Click **+ Select groups to include**.  Type **Sales** and select it.  Click **Select**.   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Confirm the URI Configurations are Applied | 1. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Select **Connected to <CompanyName> MDM** then click **Info**. 4. Click **Sync** to force a policy update and confirm that the sync was **successful**. 5. Note that when you click **Cortana** on the task bar, it says “**Cortana is disabled. To use Cortana you need to get permission from your administrator**”. |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure Windows Defender | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. On the left navigation bar, click **All services > search and click Intune > Intune**. 3. Select **Device configuration** > **Profiles** > **+** **Create profile**. 4. Under **Platform**, select **Windows 10 and later**. 5. Under **Profile type**, select **Custom** and click **Create**. 6. Under the **Basics** tab, enter the following information and click **Next**:   In the **Name** field, type **Allow Real Time Protection on Win 10 Desktops**.   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Click **Add**.  In the Name field type **Allow Real Time Protection on Win 10 Desktops**.  In the **OMA-URI** field enter (Case sensitive and starting with a period):  **./Vendor/MSFT/Policy/Config/Defender/AllowRealtimeMonitoring**  For **Data type** select **Integer**.  For **Value** enter **1** (1 means the setting is allowed).  Click **Add**.   1. Under the **Assignments** tab, enter the following information and click **Next**:   Click **+ Select groups to include**.  Type **Sales** and select it.  Click **Select**.   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Configuration is Applied | 1. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Select **Connected to <CompanyName> MDM** then click **Info**. 4. Click **Sync** to force a policy update and confirm that the sync was **successful**. 5. In the **Settings** app, go back to **Update & Security > Windows Security** and click **Open Windows Security**. 6. In the **Windows Security** app, navigate to **Virus & threat protection** and click **Manage settings** under **Virus & threat protection settings**. 7. Confirm that the **Real-time protection** setting is turned **On** and **greyed out** which shows enforcement of the policy after sometime. |

### Dynamic Management with Windows 10

In this lab, you will set up and configure dynamic management policies for Windows 10. For a list of available dynamic management policies, visit: <https://docs.microsoft.com/en-us/windows/client-management/mdm/dynamicmanagement-csp>.

**Note:** If any of the below policies conflicts with the policies from the previous labs, delete the policies from the previous labs.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure Dynamic Management Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Select **Device configuration** > **Profiles** > **+** **Create profile**. 6. Under **Platform**, select **Windows 10 and later**. 7. Under **Profile type**, select **Custom** and click **Create**. 8. Under the **Basics** tab, enter the following information and click **Next**:   In the **Name** field, type **DisableCameraInCorporateNetwork**.   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Click **Add**.  In the **Name** field enter **SettingsPack**.  In the **OMA-URI** field enter (Case sensitive and starting with a period):  **./Vendor/MSFT/DynamicManagement/Contexts/NetworkBased/SettingsPack**  For **Data type** select **String**.  For **Value** enter  **<SyncML>**  **<SyncBody>**  **<Replace>**  **<CmdID>1331</CmdID>**  **<Item>**  **<Target>**  **<LocURI>./Vendor/MSFT/Policy/Config/Camera/AllowCamera</LocURI>**  **</Target>**  **<Meta>**  **<Format xmlns="syncml:metinf">int</Format>**  **</Meta>**  **<Data>0</Data>**  **</Item>**  **</Replace>**  **<Final/>**  **</SyncBody>**  **</SyncML>**  Click **Add**.  Click **Add** again.  In the **Name** field enter **SignalDefinition**.  In the **OMA URI** field enter (Case sensitive and starting with a period):  **./Vendor/MSFT/DynamicManagement/Contexts/NetworkBased/SignalDefinition**  For **Data type** select **String**.  For **Value** enter  **<rule schemaVersion="1.0">**  **<signal type="ipConfig">**  **<ipv4Gateway>10.0.0.254</ipv4Gateway>**  **</signal>**  **</rule>**  Click **Add**.  Click **Add** again.  In the **Name** field enter **NotificationsEnabled2**.  In the **OMA-URI** field enter (Case sensitive and starting with a period):  **./Vendor/MSFT/DynamicManagement/NotificationsEnabled**  For **Data type** select **Boolean**.  For **Value** select  **True**  Click **Add**.   1. Under the **Assignments** tab, enter the following information and click **Next**:   Click **+ Select groups to include.**  Type **Sales** and select it.  Click **Select**.   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Policy is Applied | 1. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Select **Connected to <CompanyName> MDM** then click **Info**. 4. Click **Sync** to force a policy update and confirm that the sync was **successful**. 5. From the **Virtual Machine Connection** window, got to **File > Settings**. 6. In the **Settings** window, under **Network Adapter**, disable the **Corpnet Virtual Switch**. 7. In the **Settings** app, go back to **Privacy > Camera**.   **Note**: Camera is currently turned On and unmanaged because the machine is in the internet network after sometime.   1. From the **Virtual Machine Connection** window, go to **File > Settings**. 2. In the **Settings** window, under **Network Adapter**, disable the **External** **Virtual Switch** and enable the **Corpnet Virtual Switch**. 3. In the **Settings** app, refresh the **Privacy > Camera** view. 4. Confirm **\*Some of these settings are hidden or managed by your organization** is shown after sometime.   **Note**: Camera is turned Off and fully managed because the machine is in the corporate network after sometime. |

### Mobile App Management for Non-Managed Windows 10 Devices

The Windows version of mobile application management (MAM) is a lightweight solution for managing company data access and security on personal devices. MAM support is built into Windows on top of Windows Information Protection (WIP), starting in Windows 10.

In this lab, you will set up and configure Mobile App Management for an unmanaged Windows 10 device.

**Note:** If any of the below policies conflicts with the policies from the previous labs, delete the policies from the previous labs.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure MAM Service | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory** > **Mobility (MDM and MAM**) > **Microsoft Intune**. 5. In the **MAM User scope** setting, select **All**. 6. Click **Save**. |
| Configure MAM Policy | 1. Select **All services** > **search and click Intune App Protection** > **Intune App Protection** > **App protection policies**. 2. Click **+ Create policy | Windows 10**. 3. Under the **Basics** tab, in the **Name** field type **Windows 10 MAM** and select **Without enrollment** next to **Enrollment state**. Click **Next**. 4. Under the **Targeted apps** tab, under **Protected apps**, click **+ Add**. 5. In the **Add apps** pane, select **Microsoft Edge**, **IE11** and **Notepad** then click **OK**. 6. Under the **Protected apps**, confirm that the selected apps are listed then click **Next**. 7. Under the **Required settings** tab, select **Block** next to **Windows Information Protection mode** and click **Next**. 8. Under the **Advanced settings** tab, click **+ Add** under **Network perimeter**. 9. In the **Add network boundary** pane, enter the following then click **OK**.   BOUNDARY TYPE: **Cloud resources**  NAME: **SharePoint online**  VALUE: **<AzureDomainName>.sharepoint.com**   1. Under the **Advanced settings** tab, next to **Show the enterprise data protection** **icon**, click **On** and then click **Next**. 2. Under the **Assignments** tab, click **Next**. 3. Under the **Review + create** tab, click **Create**. |
| Deploy MAM Policy | 1. Select **Windows 10 MAM** > **Properties**. Scroll down and click **Edit** next to **Assignments**. 2. Click **+ Select groups to include**. 3. In the **Select groups to include** pane, enter **Sales**, select it and then click **Select**. 4. Click **Review + Save** and then click **Save**. |
| **Complete these steps on the CLIENT4 virtual machine (Note that this machine should not be Azure AD Joined or Intune Enrolled for this Lab)** | |
| Create Test File | 1. Log in to the virtual machine as **.\Administrator**. 2. Right-click on the desktop and select **New > Text Document**. 3. Rename the file to **Sample Document**. 4. Open **Sample Document.txt**. 5. In the **Notepad** window, enter **This is a sample corporate file.** then click **Save**. 6. **Close** the file. 7. Open **Internet Explorer** and navigate to **https://<AzureDomainName>.sharepoint.com**. 8. **Sign** in as **TU2@<AzureDomainName>.onmicrosoft.com**. 9. On the top, click **Documents**. 10. From the desktop, **drag** and **drop** the **Sample Document.txt** file into the Documents library to **upload** the file. 11. Once uploaded, **delete** the **Sample Document.txt** file from the **Desktop**. 12. Close all browser windows. |
| Connect Corporate Account | 1. Click **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Click **Connect**. 4. In the **Set up a work or school account** pane, enter **TU2@<AzureDomainName>.onmicrosoft.com** then click **Next**. 5. Enter the **password** then click **Sign in**. 6. In the **Help us protect your account** pane, click **Set it up now** then configure the verification requirements. 7. In the **Create a PIN** pane, click **Create PIN** then configure the Pin.   **Note**: Additional verification may be required.   1. Click **Next**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Select **Work or school account** then click **Info**. 4. Click **Sync** to force a policy update and confirm that the sync was **successful**. |
| Verify MAM Policies | 1. Open **Internet Explorer** and navigate to **https://<AzureDomainName>.sharepoint.com**. 2. **Sign** in as **TU2@<AzureDomainName>.onmicrosoft.com**.   **Note**: “.<AzureDomainName>.sharepoint.com” is protected and selected both IE11 and Microsoft Edge (they’re both enlightened apps) therefore a briefcase icon is shown in the address bar to indicate that it is protected. When the browser or another tab navigate away from this site, the briefcase will go away.   1. On the top, click **Documents**. 2. Select **Sample Document.txt** and click **Download**. 3. Save the file to the **Documents** folder.   **Note**: The briefcase icon under File Name indicates that the file is protected.   1. In the taskbar, open **File Explorer** and browse to the **Documents** folder.   **Note**: The briefcase icon in the file icon and the <AzureDomainName> under the File ownership column indicates that the file is protected.   1. **Open** the **Sample Document.txt** file using **Notepad**. The file should open because Notepad is a managed app (policy).   **Note**: The briefcase icon beside the minimize button indicates that the file is protected.   1. **Close** Notepad. 2. **Open** the **Sample Document.txt** file using **WordPad**. The file will not open and a dialog box will show up to indicate that access to the file is denied.   **Note**: WordPad is not a managed app therefore will not be able to open protected files.   1. **Close** WordPad. 2. In the **Documents** folder, **right-click** on **Sample Document.txt** and select **File ownership**.   **Note**: The Personal option is currently disabled because the policy is configured to hide overrides. If the policy is configured to allow overrides, users can remove protection from the file by selecting Personal. |

## Servicing Windows 10 with Configuration Manager

Windows 10 delivers a new model for organizations to deploy and upgrade Windows by providing updates to features and capabilities through a continuous process. Configuration Manager provides a window of the state of Windows in your environment, create servicing plans to form deployment rings and ensure that the Windows 10 machines are kept up to date.

In this section, you will go through how to configure Configuration Manager to support the new model of Windows as a Service.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

### Configure Software Update Point

In this activity, you will configure the Software Update Point to download Windows 10 Servicing Feature Updates.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure Software Update Point Site Component | 1. Open the **Configuration Manager Console** from the Start Menu. 2. Browse to **Administration > Site Configuration >** **Sites**. 3. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components >** **Software Update Point**. 4. On the **Classifications** tab, uncheck **Services Packs** and **Update Rollups** in case they are checked and then keep **Updates** selected (if it is selected from the previous lab) and check **Upgrades**. 5. On the **Windows 10 Servicing Prerequisite** window, click **OK**. 6. On the **Products** tab, uncheck everything and only check **Windows 10, version 1903 and later** and keep **Office 365 Client** selected (if it is selected from the previous lab). 7. On the **Languages** tab, uncheck everything and only check **English** (if not done before) then click **Apply** and **OK**. |
| Synchronize Software Update | 1. From the **Configuration Manager Console**, browse to **Software Library > Software Updates > All Software Updates**. 2. Click **Synchronize Software Updates**. 3. On the **Configuration Manager** dialog box, click **Yes**.   **Note**: The synchronization may take 30 minutes or more depending on the speed of the internet connection. |

### Configure Servicing Plan

In this activity, you will configure Servicing Plans in Configuration Manager to form deployment rings and ensure that Windows 10 systems are kept up to date when new builds are released.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Validate that Windows 10 Feature Updates are Available | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing >** **All Windows 10 Updates**. 2. On the **Search** bar, type **Feature update to Windows 10 (business editions), version 21H1, en-us x64** then press **Enter**. 3. Validate that the feature update metadata for **Feature update to Windows 10 (business editions), version 21H1, en-us x64** is available and showing in a state of **“Required”**.   **Note:** It can take some time for the **WIN10-20H2** machine to be detected in Configuration Manager for the **“Required”** update. Run **Hardware Inventory Cycle**, **Machine Policy Retrieval & Evaluation Cycle**, **Software Inventory Cycle**, **Software Updates Deployment Evaluation Cycle** and **Software Updates Scan Cycle** on the machine to fasten the process. |
| Create Servicing Collections | 1. From the **Configuration Manager Console**, browse to **Assets and Compliance**. 2. Right-click on **Device Collections** and select **Folder >** **Create Folder**. 3. On the **Configuration Manager** window, under **Folder name** enter **Windows 10 Servicing** then click **OK**. 4. From the **Configuration Manager Console**, expand **Device Collections** and right-click on **Windows 10 Servicing**. 5. Select **Create Device Collection**. 6. On the **General** page, enter the following then click **Next**.   Name: **Semi-Annual Channel**  Limiting Collection: **All Desktop and Server Clients**   1. On the **Membership Rules** page, click **Next**. 2. On the warning dialog box, click **OK**. 3. On the **Summary** page, click **Next**. 4. On the **Completion** page, click **Close**. |
| Create a Servicing Plan for Semi-Annual Channel Machines | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing > Servicing Plans**. 2. On the ribbon, click **Create Servicing Plan**. 3. On the **General** page, enter the following then click **Next**.   Name: **Semi-Annual Channel**   1. On the **Servicing Plan** page, enter the following then click **Next**.   Target Collection: **Semi-Annual Channel** (under Windows 10 Servicing folder)   1. On the **Deployment Ring** page, select **Semi-Annual Channel (Targeted)**, and then click **Next**. 2. On the **Upgrades** page, select **Title** and click **items to find**. 3. On the **Search Text** window, in the textbox enter **“Feature update to Windows 10 (business editions), version 21H2, en-us x64”** (include the quotation marks) then click **Add**. 4. On the **Search Text** window, click **OK**. 5. On the **Upgrades** page, click **Preview**. 6. On the **Preview updates** window, verify that the **21H1** feature update is listed then click **Close**. 7. On the **Upgrades** page, click **Next**. 8. On the **Deployment Schedule** page, under **Installation deadline** select **As soon as possible** then click **Next**. 9. On the **User Experience** page, under **User notifications** select **Display in Software Center and show all notifications**,under **Deadline behavior** select **System restart (if necessary)** and then click **Next**. 10. On the **Deployment Package** page, select **Create a new deployment package**, enter the following then click **Next**.   Name: **Semi-Annual Channel Package**  Package source: **\\CM1\Packages$\SACPackage**  **Note:** Create a folder called **SACPackage** in **C:\Packages**.   1. On the **Distribution Points** page, click **Add >** **Distribution Point**. 2. On the **Add Distribution Points** window, select **CM1.CORP.CONTOSO.COM** then click **OK**. 3. On the **Distribution Points** page, click **Next**. 4. On the **Download Location** page, click **Next**. 5. On the **Language Selection** page, click **Next**. 6. On the **Summary** page, click **Next**. 7. On the **Completion** page, click **Close**. |

### Service a Windows 10 20H2 Client

In this activity, you will test the servicing plan on a Windows 10 20H2 virtual machine.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Move the Test Device to Semi-Annual Channel Collection | 1. From the **Configuration Manager Console**, browse to **Assets and Compliance >** **Devices**. 2. Right-click on **WIN10-20H2** and select **Add Selected Items >** **Add Selected Items to Existing Device Collection**. 3. On the **Select Collection** window, browse to and select **Root > Windows 10 Servicing >** **Semi-Annual Channel** then click **OK**. 4. On the **Configuration Manager Console**, browse to **Assets and Compliance > Device Collections > Windows 10 Servicing > Semi-Annual Channel**. 5. On the ribbon, click **Collection |** **Update Membership | Yes** and press **F5**. 6. Verify that the **WIN10-20H2** machine is shown within the collection. |
| Force the Servicing Plan to Run | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing >** **Servicing Plans**. 2. Select **Semi-Annual Channel** and from the ribbon click **Run Now**. 3. On the dialog box, click **OK**. |
| **Complete these steps on the WIN10-20H2 virtual machine.** | |
| Refresh the Client’s Policy | 1. Logon to **WIN10-20H2** machine as **corp\labadmin**. 2. Open the **Control Panel**. 3. On the **All Control Panel Items** window, click on **Configuration Manager.** 4. On the **Configuration Manager Properties** window, go to the **Actions** tab. 5. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** then click **Run Now**. 6. On the dialog box, click **OK**. 7. On the **Actions** tab, select **Software Updates Scan Cycle** then click **Run Now**. 8. On the dialog box, click **OK**. 9. On the **Actions** tab, select **Software Updates Deployment Evaluation Cycle** then click **Run Now**. 10. On the dialog box, click **OK**. 11. On the **Configuration Manager Properties** window, click **OK**.   **Note:** Ensure that in **CM1**, the option **Download software updates from distribution point and install** is selected **in all cases** in the **Servicing Plan Properties** under **Download Settings** as well as in the **Software Update Group’s**, **Deployment Properties** under **Download Settings**.   1. A notification will appear after which once the **Software Center** is launched, under the **Installation Status**, the feature update will start **downloading** and **Installing** automatically. 2. On the prompt, click **Restart** and then click **Restart** again for a force restart. 3. The upgrade process will continue. 4. Once restarted and logged in, the version of windows will be **Windows 10 Version 21H1 (Build 19041.x)**. |

## Servicing Microsoft 365 Apps for enterprise using Configuration Manager

In this section, you will go through how to configure Configuration Manager to support Office updates.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

### Enable Configuration Manager to receive Microsoft 365 Client Package Notifications

To start, you need to configure Configuration Manager to receive notifications when Microsoft 365 client update packages are available.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
|  | 1. In the Configuration Manager console under the **Administration** node, choose **Site Configuration > Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components > Software Update Point**. 3. In the **Software Update Point Component Properties** dialog box, do the following:    1. On the **Products** tab, under **Office**, select **Office 365 Client** (if not already selected from the previous labs).    2. On the **Classifications** tab, select **Updates** (if not already selected from the previous labs).    3. Click **Apply** and **OK**.   You can have other checkboxes selected in the Products and Classifications tabs. But, **Office 365 Client** and **Updates** need to be selected for Configuration Manager to receive notifications when Microsoft 365 client update packages are available.   1. On the **Software Library** node, open **Office 365 Client Management** and right-click **Office 365 Updates** and select **Synchronize Software Updates.** 2. On the **Configuration Manager** dialog box, click **Yes**.   **Note:** The synchronization may take 30 minutes or more depending on the speed of the internet connection. |

### Enable Office COM Objects to Manage Microsoft 365 Client Updates

For Configuration Manager to be able to manage Microsoft 365 client updates, an Office COM object needs to be enabled on the computer where Office is installed. The Office COM object takes commands from Configuration Manager to download and install client updates.

You can enable the Office COM object by using either the Office Deployment Tool or Group Policy.

This lab guide will use Group Policy to enable Office COM Objects. This does the same thing as setting the OfficeMgmtCOM attribute to True in the configuration.xml file used by the Office Deployment Tool. But, with Group Policy, you can apply this setting to multiple computers, an organizational unit (OU), or a domain.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Download ADMX Files (If not downloaded before in the previous labs) | 1. Download the Office 2016 Administrative Template files (ADMX/ADML)   <https://www.microsoft.com/download/details.aspx?id=49030>  **Note:** Download the appropriate version for the Office architecture you support. In this lab download the x64 version. |
| Install ADMX Files (If not installed before in the previous labs) | 1. Install **admintemplates\_x64\_<VersionNumber>\_en-us.exe** to temporary location. 2. **Copy** contents of **admx** folder in temporary location to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**.   **Note:** If PolicyDefinitions folder doesn’t exist you will have to create it and also copy in the latest Windows 10 ADMX files.  [Download Administrative Templates (.admx) for Windows 10 October 2020 Update (20H2) - v2.0 from Official Microsoft Download Center](https://www.microsoft.com/en-us/download/details.aspx?id=103060)  (Will have a link to latest ADMX files).  **Note:** Version number may change over time. |
| Enable Microsoft 365 Clients to receive Updates from ConfigMgr | 1. Open the Group Policy Management Console. 2. Create a policy called “**Microsoft 365 Client Management**". 3. Edit the “**Policy**”. 4. Enable the **Computer Configuration\Policies\Administrative Templates\Microsoft Office 2016 (Machine)\Updates\Management of Microsoft 365 Apps for enterprise** policy setting. 5. Link the GPO to the OU containing the clients.   **Note:** Create a temporary OU called **Microsoft 365** and move **CLIENT1** or **CLIENT2** there. Run a **gpupdate /force** on the clients. Remember to move these clients back to the default **Computers** container after the lab is done. |

### Configure Office Updates

**Note:** Before deploying Microsoft 365 Updates to CLIENT1 or CLIENT2 VMs from Configuration Manager, ensure that the Configuration Manager Client is installed. For versions released as per channels, refer to <https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date>

| Task | | Detailed Steps | | |
| --- | --- | --- | --- | --- |
| **Complete these steps on the CLIENT1 or CLIENT2 virtual machine.** | | | | |
| Download Office Deployment Tool | | 1. Logon as a corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. | | |
| Extract ODT | | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. | | |
| Create Installation XML | | 1. The Sample Configurations for all Office Applications – Current Channel from the <https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool> can be referenced. 2. Open Internet Explorer and browse to the URL below. [https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date](https://technet.microsoft.com/en-us/library/mt592918.aspx) 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, select **Microsoft Endpoint Configuration Manager**. 7. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 8. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. | | |
| Deploy Microsoft 365 Apps | | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. | | |
| **Complete these steps on the CM1 virtual machine.** | | | |
| Validate that Microsoft 365 Apps Updates are Available | 1. From the **Configuration Manager Console**, browse to **Software Library > Office 365 Client Management >** **Office 365 Updates**. 2. Search for **the latest MC Version**. You should be able to see **the latest MC Version** showing in a state of **“Required”** as per <https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date?redirectSourcePath=%252fen-us%252farticle%252fae942449-1fca-4484-898b-a933ea23def7>   **Note:** It can take some time for the **CLIENT1** or **CLIENT2** machines to be detected in Configuration Manager for the **“Required”** update. Run **Hardware Inventory Cycle**, **Machine Policy Retrieval & Evaluation Cycle**, **Software Inventory Cycle**, **Software Updates Deployment Evaluation Cycle** and **Software Updates Scan Cycle** on the machines to fasten the process. | | |
| Create Servicing Collections | 1. From the **Configuration Manager Console**, browse to **Assets and Compliance**. 2. Right-click on **Device Collections** and select **Folder >** **Create Folder**. 3. On the **Configuration Manager** window, under **Folder name** enter **Microsoft 365 Apps Updates** then click **OK**. 4. From the **Configuration Manager Console**, expand **Device Collections** and right-click on **Microsoft 365 Apps Updates**. 5. Select **Create Device Collection**. 6. On the **General** page, enter the following then click **Next**.   Name: **Microsoft 365 Apps Current Channel**  Limiting Collection: **All Desktop and Server Clients**   1. On the **Membership Rules** page, click **Next**. 2. On the warning dialog box, click **OK**. 3. On the **Summary** page, click **Next**. 4. On the **Completion** page, click **Close**. | | | | |
| Add Devices to Collections | 1. Right-click **Microsoft 365 Apps Current Channel** collection and click **Add Resources.** 2. In the **Add Resources to Collection** enter **CLIENT1** or **CLIENT2** in the **Name string contains** field then click **Search**. 3. In the **Search results** box, select **CLIENT1** or **CLIENT2** and click **Add** then **OK**. | | | | |
| Create ADR for Current Channel | 1. Browse to **Software Library**. 2. Click on the **Office 365 Client Management** and then click **Create an ADR**. | | | | |
| General Page | | 1. Fill out as defined below and click **Next**:   **Name:** Microsoft 365 Apps Updates – Current Channel  **Template:** Office 365 Client Updates  **Collection:** Microsoft 365 Apps Current Channel | | |
| Deployment Settings | | 1. Keep defaults and click **Next**. | | |
| Software Updates | | 1. Fill out as defined below and click **Next**:   **Product:** Office 365 Client  **Title:** “Office 365 Client Update…” (Full title of the update) | | |
| Evaluation Schedule | | 1. Fill out as defined below and click **Next**:   **Run the rule on a schedule:** Selected  **Schedule:** Occurs day 15 of every 1 month | | |
| Deployment Schedule | | 1. Fill out as defined below and click **Next**:   **Software available time:** As soon as possible  **Installation deadline:** As soon as possible | | |
| User Experience | | 1. Select **Display in Software Center and show all notifications** and click **Next**. | | |
| Alerts | | 1. Keep defaults and click **Next**. | | |
| Deployment Package | | 1. Fill out as defined below and click **Next**:   **Create a new deployment package:** Selected  **Name:** Microsoft 365 Apps Updates  **Package Source:** \\CM1\Packages$\Microsoft365AppsUpdates  **Note:** Create the folder beforehand. | | |
| Distribution Point | | 1. Fill out as defined below and click **Next**:   **Distribution Point Group:** Corp DPs | | |
| Download Location | | 1. Keep defaults and click **Next**. | | |
| Language Selection | | 1. Keep defaults and click **Next**. | | |
| Download Settings | | 1. Keep defaults and click **Next**. | | |
| Summary | | 1. Click **Next**. | | |
| Completion | | 1. Click **Close**. | | |
| Run ADRs | 1. Open **Software Updates\Automatic Deployment Rules**. 2. Right-click **Microsoft 365 Apps Updates – Current Channel** and click **Run Now**. Click **OK**. | | | | |
| **Complete these steps on the CLIENT1 or CLIENT2 virtual machine.** | | | | | |
| Apply Updates | 1. In the **Configuration Manager Properties**, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**. 4. The software update will start **Downloading** and **Installing**.   The installation of the package can be validated in the **Programs and Features**. | | | | |

### Cloud-Based Policy Management Service for Microsoft 365 Apps for enterprise

The Office cloud policy service helps administrators manage policies for all Microsoft 365 Apps for enterprise users in their organization, from an easy-to-use, Internet-based portal focused on Microsoft 365 Apps management.

Microsoft 365 Apps allows users to access full Office experiences from multiple Windows devices. These may be managed or MDM-enrolled devices, but are often also personally-owned and unmanaged. Now with the Office cloud policy service, you can define and enforce Office policies without the infrastructure or MDM services traditionally required.

The office cloud policy services allows administrators to define policies for Microsoft 365 Apps and assign these policies to users via Azure Active Directory security groups. Once defined, these office policies are automatically enforced as users sign in and use Microsoft 365 Apps.

* **Build a policy configuration** that includes the policies you want to enforce, configured as needed for your organization’s needs. The service is always up to date and includes the latest policies as they are released.
* **Target a group of users** by assigning a policy configuration to a specific AAD security group.
* **Policies automatically enforced** as users sign into Microsoft 365 Apps.

This service compliments Group Policy-based management as another option. Group Policy management enforces policies on Windows PCs joined to an Active Directory domain, while the Office cloud policy service only requires Azure Active Directory sign-in as part of Microsoft 365 Apps.

Office Cloud policy service manages user-based policies for Microsoft 365 Apps. Group Policy can manage both user-based and machine-based policies.

The settings configured as part of Office installation using the Office Customization Tool for Click-to-Run – as well as previous OCT versions – are based on ‘preferences’, meaning that a user can change them. Office cloud policy service settings are enforced, similar to Group Policy enforcement.

It is not required that the tenant have an Intune subscription. This is a feature of Microsoft 365 Apps and only requires that the tenant have a subscription that includes Microsoft 365 Apps.

This is a feature of Microsoft 365 Apps and only works with the Office apps that are deployed as a part of the Microsoft 365 Apps suite.

It is right now limited to a subset of the user based policies defined in the ADMX templates. All machine based policies are not included.

Only the Global Admin, Security Admin or Desktop Analytics Admin (private preview) roles are allowed access to create or view policy configurations.

For more information on Cloud-Based Policy Management Service for Microsoft 365 Apps, refer to <https://techcommunity.microsoft.com/t5/Office-365-Blog/Announcing-the-new-cloud-based-policy-management-service-for/ba-p/310405> and <https://docs.microsoft.com/en-us/DeployOffice/overview-office-cloud-policy-service>

**Prerequisites:**

1. At least version 2004 or 2005 of Microsoft 365 Apps installed. In **CLIENT3** or **CLIENT4** ensure that the latest version of Microsoft 365 Apps is installed from <https://portal.office.com> and **CLIENT3** or **CLIENT4** are Azure Active Directory Joined and enrolled into Intune with the user (**TU1 or Test User1**).
2. User accounts created in or synchronized to Azure Active Directory (AAD). The user (**TU1 or Test User1**) must be signed into Microsoft 365 Apps with an AAD-based account, example: **TU1@<AzureDomainName>.onmicrosoft.com**
3. Security groups created in or synchronized to Azure Active Directory (AAD), with the appropriate users added to those groups. Created as part of this lab.
4. To create a policy configuration, you must be assigned one of the following roles in Azure Active Directory (AAD): Global Administrator, Security Administrator, or Desktop Analytics Administrator. We will be using **LabAdmin@<AzureDomainName>.onmicrosoft.com**, which is a Global Administrator.

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | | | |
| Create a Security Group | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:    * 1. GROUP TYPE: **Security**      2. GROUP NAME: **OCPSDemo**      3. MEMBERSHIP TYPE: **Assigned**      4. MEMBERS: **TU1,TU2** 4. Click **Create**. | | |
| Create a Policy Configuration | 1. Navigate to <https://config.office.com/> and sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. Now under **Customization**, go to **Policy management** and click **Create**. 2. Provide a **Name** - **OCPSDemo** an optional **Description** and click **Assignments**. 3. Select **This policy configuration applies to users** and then click **Select Group**. 4. Search for and select **OCPSDemo** and then click **Configure Policies**. 5. Search for **Macros**. 6. Click **Block macros from running in Office files from the Internet** for the **Word** application. 7. Under **Policy type**, select **Microsoft recommended security baseline**. 8. Ensure that under **Configured**, Enabled is the option **selected**. Click **OK**. 9. Once done, click **Create**. | | |
| **Complete these steps on the CLIENT3 or CLIENT4 virtual machine.** | | | |
| User Policy on the Client | 1. When a user signs into Office on a device for the first time, a check is immediately made to see   if there is a policy configuration that pertains to the user. If the user is a member of an AAD group  that is assigned a policy configuration, then the appropriate policy settings are applied. | | |

## Servicing Microsoft 365 Apps for enterprise using Intune

In Intune, you can use [Windows 10 templates to configure group policy settings](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows). This section shows you how to update Microsoft 365 Apps using an administrative template in Intune.

In this scenario, you create an administrative template in Intune that updates Microsoft 365 Apps on your devices.

For more information on administrative templates, see [Windows 10 templates to configure group policy settings](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows).

For more information on how to Use Update Channel and Target Version settings to update Microsoft 365 Aps with Microsoft Intune Administrative Templates, refer to - <https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-update-office>

**Note:** In order to test Microsoft 365 Apps Updates with Intune, on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Profiles/Policies from the previous labs. Also, install an earlier version of Microsoft 365 Apps.

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | | | |
| Prerequisites | 1. Be sure to [enable Microsoft 365 Apps Automatic Updates](https://docs.microsoft.com/en-us/deployoffice/configure-update-settings-for-office-365-proplus) for your Office apps.   You can do this using group policy, or the Intune Office 2016 ADMX template. | | |
| Set the Update Channel in the Intune Administrative Template | 1. In your [Intune administrative template](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows#create-the-template), go to the **Update Channel** setting, and enter the   channel you want. For example, choose **Current Channel**.   1. Be sure to [assign the policy](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign) to your Windows 10 devices. To test your policy sooner, you   can also sync the policy:   * [Sync the policy in Intune](https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-sync) * [Manually sync the policy on the device](https://docs.microsoft.com/en-us/mem/intune/user-help/sync-your-device-manually-windows#sync-from-settings-app) | | |

## Security and Compliance

In this module, you will go through Windows 10 capabilities that could help organizations be more secure. We will cover the following scenarios:

* BitLocker device encryption
* Windows Defender Antivirus
* Windows Hello for Business
* BIOS to UEFI conversion as an enabler for virtualization-based security
* Windows Defender Credential Guard
* Windows Defender Application Guard
* Windows Defender Exploit Guard
* Windows Defender Application Control
* Windows Defender Advanced Threat Protection

**Note:** In the Security Module, you will need the vTPM enabled on Client VMs in many scenarios. In order to enable vTPM on Client VMs, the Hyper-V Configuration Version must be at **8.0** in Windows Server 2016 Hyper-V Host for **HYD-CLIENT 1, 2, 3 and 4**. Also, you will notice that **HYD-CLIENT 1, 2, 3 and 4** are **GEN1** VMs. In order to enable vTPM on Client VMs, these **GEN1** VMs need to be converted to **GEN2** VMs.

Now, in order to enable vTPM on the Client VMs, perform the following steps:

**Note: (x) = 1, 2, 3 and 4.**

1. In Hyper-V Manager, turn on **HYD-CLIENT(x)** and log in. In **HYD-CLIENT(x)**, open an **elevated command prompt**.
2. Type **cd C:\Windows\System32** and press **Enter**.
3. Now type, **MBR2GPT.EXE /convert /AllowFullOS** and press **Enter**.
4. Once the conversion process completes, **shut down the VM**.
5. In Hyper-V Manager, select **HYD-CLIENT(x)** and click **Delete** under the **Actions** pane on the right.
6. Click **Delete** again on the Delete Selected Virtual Machines dialog box.
7. On the right, under the **Actions** pane, click **New > Virtual Machine…**
8. On the Before You Begin page, click **Next**.
9. On the Specify Name and Location page, for **Name**, enter **HYD-CLIENT(x)** and click **Next**.
10. Now, on the Specify Generation page, select **Generation 2** and click **Next**.
11. On the Assign Memory page, for **Startup memory**, provide a memory of **2GB or more** and click **Next**.
12. On the Configure Networking page, for **Connection**, select **HYD-CorpNet** and click **Next**.
13. On the Connect Virtual Hard Disk page, select **Use an existing virtual hard disk**, **Browse…** to the **SelfService** folder which contains the Lab Kit files and select **HYD-CLIENT(x).VHDx**. Click **Open** and click **Next**.
14. On the Completing the New Virtual Machine Wizard page, click **Finish**.
15. Now select the newly created **HYD-CLIENT(x)** and on the right under the **Actions** pane, click **Settings...**
16. Click **Security** and under **Secure Boot**, ensure that **Enable Secure Boot** is checked.
17. Under **Security**, under **Encryption Support**, check **Enable Trusted Platform Module**.
18. Click **Apply | OK**.
19. **Turn on the VM** to ensure that the VM is turning on and are able to log in and then **shut the VM back down**.
20. These **Steps 1-19** must be performed for **HYD-CLIENT 1, 2, 3 and 4**.

**Note:** In order to avoid hiccups during “Modern Management” scenarios using Intune, if you have been using **CLIENT3** and **CLIENT4** as Azure AD Joined or Enrolled to MDM Only in other Labs, recommend you to disjoin the machines from Azure AD or Un-enroll the machines from MDM, cleanup these two computer objects from Azure AD and Intune Portals and then re-join them to Azure AD using **TU2@<AzureDomainName>.onmicrosoft.com**. They will get automatically enrolled to Intune as well.

**Note:** In order to see immediate effects of Intune policies after running a sync, reboot the machine or shut down and then start the machine. It may take few minutes for the policies to be applied on the machine from Intune.

### BitLocker

In this section, we will walk you through setting up BitLocker using modern and on-premises management.

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

On computers that do not have a TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the operating system volume on a computer without TPM. Both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive, that contains a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is presented.

#### Cloud Management.

The below section will walk you through setting up BitLocker with Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Groups | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **BitLockerDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1, TU2**   1. Click **Create**. |
| Configure Windows Bitlocker | 1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Under **Manage** select “**Device configuration**”. 5. Under **Manage** select “**Profiles**”. 6. Select “**+ Create profile**”. 7. For Platform select “**Windows 10 and later**”. 8. For Profile select “**Endpoint protection**” and click **Create**. 9. Under the **Basics** tab, enter the following and click **Next**:   Name: **Bitlocker Demo**   1. Under the **Configuration settings** tab, enter the following and click **Next**:   Expand **Windows Encryption**  Encrypt devices: **Require**  Encrypt storage card (mobile only): **Not configured**  Warning for other disk encryption: **Not configured**  Configure encryption methods: **Enable**  Encryption for operating system drives: **XTS-AES 128-bit**  Encryption for fixed data-drives: **XTS-AES 128-bit**  Encryption for removable data-drives: **AES-CBC 128-bit**  Additional authentication at startup: **Not configured**  **Note:** The rest is not going to be configured.   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **BitLockerDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Verify the Policy has been Applied and Working | 1. Log in to the machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. After a few minutes of syncing, you will notice that a notification appears **Encryption needed** (at least once) asking you to start encryption. |

#### On-Premises Method

This section describes how to install and configure MBAM server and client components. The server components can be installed using two possible topologies:

* Stand Alone
* Configuration Manager

Both of these installations include the following components: Self-Service Portal, Key Database, Reports Database, Reports, Administration Monitoring Server, Group Policy Template.

To configure MBAM the following tasks need to be performed:

1. Create a GPO to apply MBAM settings to client devices.
2. Test the configuration on a client device.
3. Connect to the Self-Service Portal.

Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Download MDOP Group Policy Templates | 1. Open Internet Explorer and browse to the URL below.   https://www.microsoft.com/en-us/download/details.aspx?id=55531   1. Click **Download** and save the **MDOP\_ADMX\_Templates.cab** file to **C:\packages**. 2. On the taskbar, open **File Explorer** and browse to **C:\packages** and create a folder named **MDOPGPO**. |

Create and Deploy MBAM Settings

This activity will guide you through creating and deploying a group policy object that will enforce the configuration of MBAM and BitLocker on the targeted devices.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Create and Deploy MBAM Policies | 1. Start **Command Prompt (Elevated)**. Accept the UAC prompt. 2. On the Command Prompt window, change the working directory to **C:\packages**. 3. On the Command Prompt window, “**manually type**” the following command and press **Enter**.   **expand MDOP\_ADMX\_Templates.cab -F:\* C:\packages\MDOPGPO**   1. Copy all the contents of **C:\packages\MDOPGPO\MBAM2.5SP1** to the Policy Central Store **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. 2. Open the **Group Policy Management** console. 3. Navigate to **Group Policy Management / Forest: corp.contoso.com / Domains /** **corp.contoso.com**. 4. Right-click **corp.contoso.com**, then click **Create a GPO in this domain, and Link it here**… 5. In the Name field type **MBAM Client Configuration**, click **OK**. 6. Expand **corp.contoso.com**, right-click on **MBAM Client Configuration** and select **Edit…** 7. Navigate to **Computer Configuration / Policies / Administrative Templates / Windows Components / MDOP MBAM (BitLocker Management)**. 8. Configure the suggested default settings as outlined in the Planning for MBAM 2.0 Group Policy Requirements Guide - <https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v2/planning-for-mbam-20-group-policy-requirements-mbam-2?redirectedfrom=MSDN>. Refer to the screenshot below for the settings.   **Note**: To utilize MBAM on a virtual machine, ensure that Allow BitLocker without a compatible TPM is checked. Ensure that group policies are updated in the **CLIENT2** virtual machine and **APP1** is up and running. |

A screenshot of a social media post

Description automatically generated

Test MBAM Configuration

This activity will guide you through the client experience of MBAM assuming control of BitLocker management.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Install MBAM Agent | 1. Install MBAM client from **\\APP1\C$\packages\Sources\MBAM 2.5 SP1\x64\MBAMClientSetup.exe**. 2. Click **Yes** on the UAC prompt if required. 3. Click **I accept** and click **Next** and complete the installation. |
| Reduce the MBAM Client Startup Delay | 1. From the **Start** screen, find and start **Regedit**. Accept the UAC prompt if required. 2. Navigate to **HKEY\_LOCAL\_MACHINE\Software\Microsoft\MBAM**. 3. Create a DWORD key named **NoStartupDelay**. 4. Set the value of **NoStartupDelay** to **1**. 5. Navigate to **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\FVE\MDOPBitLockerManagement**. 6. Update the value of **ClientWakeupFrequency** to **1**. 7. Update the value of **StatusReportingFrequency** to **1**. |
| MBAM Client | 1. Restart **CLIENT2** to force a full group policy update and **Start/Restart** the **BitLocker Management Client Service** and **Bitlocker Drive Encryption Service** from the **Services** MMC Console. 2. You will notice that a window appears asking you to start encryption in a moment. |

Connect to Self-Service Portal

The following activity may be used to demonstrate the access and use of the Self-Service portal provided by MBAM.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Access the MBAM Self-Service Portal | 1. In Internet Explorer enter the following URL **http://app1.corp.contoso.com/selfservice**, where app1.corp.contoso.com is the path to the MBAM server. 2. When prompted enter user credentials **corp\labadmin** and **P@ssw0rd** and click **OK**. 3. Review the portal. Check the box next to **I have read and understand the above notice** and click **Continue** and then review the next page. |

### Windows Defender Antivirus

Windows Defender Antivirus keeps your PC safe with trusted antivirus protection built-in to Windows 10. Windows Defender Antivirus delivers comprehensive, ongoing and real-time protection against software threats like viruses, malware and spyware across email, apps, the cloud and the web.

In this section, you can use modern or on-premises management to configure WDAV.

* + - 1. Cloud Management

In this section, you are going to configure Windows defender using Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Groups for use with Windows Defender Anti-Virus Lab | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDAVDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. |
| Creating an Intune Windows Defender Antivirus Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click **+ Create profile**. 10. In the Platform, select **Windows 10 and later**. 11. In the Profile, select “**Device restrictions**” and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**:   Name: **WDAV Demo**   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Expand **Microsoft Defender Antivirus** |
|  | Real-time monitoring: **Enable**  Behavior monitoring: **Enable**  Network Inspection System (NIS): **Enable**  Scan all downloads: **Enable**  Scan scripts loaded in Microsoft web browsers: **Enable**  End-user access to Defender: **Block**  Security intelligence update interval (in hours): **2**  Monitor file and program activity: **Monitor incoming files only**  Days before deleting quarantined malware: **90**  CPU usage limit during a scan: **10**  Scan archive file: **Enable**  Scan incoming mail messages: **Enable**  Scan removable drives during a full scan: **Enable**  Scan files opened from network folders: **Enable**  Cloud-delivered protection: **Enable**  Time extension for file scanning by the cloud: **50**  Prompt users before sample submission: **Always prompt**  Detect potentially unwanted applications: **Enable**  On Access Protection: **Block**  Actions on detected malware threats: **Enable**  Low severity: **Quarantine**  Moderate severity: **Quarantine**  High severity: **Quarantine**  Severe severity: **Quarantine**  **Note:** No exclusions will be configured   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select “**WDAVDemo**”   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Verify the Policy has been Applied and Working | 1. Log in to the machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. 9. **Reboot** the machine. 10. Log back in with the same credentials. 11. Click **Start**. 12. Type and click “**Windows Security settings**”.   **Note:** Notice that the page for **Virus & threat protection** is not available under **Protection areas** in a few moments because of the policy managing it. |

#### On-premises Method

In this section, you will use Configuration Manager to manage WDAV on clients.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Add “Endpoint Protection Role” to your Site | 1. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Administration**. 3. Expand **Site Configuration**. 4. Click on **Servers and Site System Roles**. 5. Right-click on **CM1.corp.contoso.com**. 6. Select **Add Site System Roles**. 7. Click **Next** on the Select a server to use as a site system. 8. Click **Next** on the Specify Internet proxy server. 9. Check **Endpoint Protection point**. 10. Click **OK**. 11. Click **Next**. 12. Select **Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)**. 13. Click **Next**. 14. Click **Next**. 15. Click **Close**. |
| Enable Configuration Manager to Manage Client Endpoint Protection | 1. Click **Administration**. 2. Click on **Client Settings**. 3. Right-click on **Default Client Settings**. 4. Click on **Properties**. 5. Click on **Endpoint Protection**. Click **OK** if a prompt comes. 6. Change **Manage Endpoint Protection client on client computers** to **Yes**. 7. Click on **OK**. |
| Create a Collection | 1. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Assets and Compliance**. 3. Click on **Devices**. 4. Right-click on **CLIENT1**. 5. Click on **Add Selected Items**. 6. Select **Add Selected Items to New Device Collection**. 7. Enter **WDAV Client1** for the collection name. 8. Limit collection to **All Desktop and Server Clients**. 9. Select **Next**. 10. Select **Next**. 11. Select **Next**. 12. Select **Close**. |
| Create a Custom Antimalware Policy | 1. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Assets and Compliance**. 3. Expand on **Endpoint Protection**. 4. Click on **Antimalware Policies**. 5. Click on **Create Antimalware Policy**. 6. Fill out the form:   Name: **WDAV Demo Policy**  Description: **WDAV Demo Policy**  Check the following boxes:  **Schedule scans**  **Scan settings**  **Default actions**  **Real-time protection**  **Exclusion settings**  **Advanced**  **Threat overrides**  **Cloud Protection Service**  **Security Intelligence updates**   1. Click on **OK**. 2. Right-click on **WDAV Demo Policy**. 3. Click **Deploy**. 4. In the right-hand corner, click on **WDAV Client1**. 5. Click **OK**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Check Policy Configuration | 1. Open **Control Panel**. 2. Search for **Configuration Manager**. 3. Open **Configuration Manager**. 4. Click on the **Actions** Tab. 5. Click on **Machine Policy Retrieval & Evaluation Cycle**. 6. Click on **Run Now**. Click **OK**. 7. Wait 3 to 5 minutes then continue. 8. Click **Start**. 9. Type **Windows Security** and click **Windows Security settings**. 10. Under **Protection areas** click **Virus & threat protection**. 11. Under **Virus and threat protection settings**, click **Manage settings**. 12. Notice the This setting is managed by your administrator. |

### Windows Hello for Business

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair.

In this lab, you will find all the information to deploy Windows Hello for Business in a Certificate Trust Model in your on-premises environment.

#### Cloud Management

The following sections cover managing Windows Hello for Business through modern management tools. In this lab we are going to setup Windows Hello for Business in the Cloud.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configuring Windows Hello for Business | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. |
|  | 1. Select “**Device enrollment**”. 2. Select “**Windows enrollment**”. 3. Select “**Windows Hello for Business**”. |
|  | 1. Select **Enabled** next to “**Configure Windows Hello for Business**”. 2. Review possible settings. 3. Select **Save**. |
| **Complete these steps on the CLIENT4 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Setting up your PIN for the First Time | 1. Log in for the first time to the virtual machine as:   **TU1@<AzureDomainName>.onmicrosoft.com**, assuming it is already Azure AD Joined and Autoenrolled into Intune.   1. Click “**Set up PIN**”. 2. Click “**Set it up now**”. 3. Select a verification method “**Text message**”. 4. Select a region that is correct for your cell phone. 5. Enter your phone number. 6. Select **Next**.   **Note:** Steps 15-19 are required only when you are setting up for the first time for a user.   1. Retrieve security code from your phone and enter it. 2. Select **Verify**. 3. Enter a new PIN “214359” (or a PIN of your choice, just don’t forget it). 4. Confirm your PIN “214359” and click **OK**. Click **OK** again. Now you will test your new PIN. 5. Sign out. 6. Sign back in using your PIN. |

### BIOS to UEFI Conversion

MBR2GPT.EXE converts a disk from Master Boot Record (MBR) to GUID Partition Table (GPT) partition style without modifying or deleting data on the disk. The tool is designed to be run from a Windows Preinstallation Environment (Windows PE) command prompt, but can also be run from the full Windows 10 operating system (OS).

You can use MBR2GPT to perform the following:

* [Within the Windows PE environment]: Convert any attached MBR-formatted disk to GPT, including the system disk.
* [From within the currently running OS]: Convert any attached MBR-formatted disk to GPT, including the system disk.

**Note**: MBR2GPT is available in Windows 10 later versions. The tool is available in both the full OS environment and Windows PE.

#### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Prerequisite Lab** | Complete **Section 9.2.4.3** Manual Upgrade |

#### Conversion after In-Place Upgrade

**Note:** This will only work if upgrade is done to Windows 10 2004 or later.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Device provided by the Customer.** | |
| Validate System Readiness | 1. **Right-click** the **Start** button and select **Disk Management**. 2. **Right-click** on **Disk 0** and select **Properties**. 3. In the **Properties** window, go to the **Volumes** tab. 4. Validate that the **Partition style** is configured as **Master Boot Record (MBR)**. 5. From the **Start** button, open an **Administrative Command Prompt** and browse to **C:\Windows\System32**. 6. **Enter** the following command:   **mbr2gpt /validate /allowFullOS**   1. Verify that the result has no errors. |
| Execute MBR2GPT Command | 1. **Enter** the following command:   **mbr2gpt /convert /allowFullOS**   1. Verify that the result has no errors. You can safely ignore the last 3 messages. |
| Reconfigure Firmware | 1. **Reboot** the device and reconfigure the **firmware** to boot in **UEFI** mode, enable **Secure Boot**, and disable **CSM** by:  * Changing the relevant settings in the firmware menu, or * Running a tool provided by the PC or firmware manufacturer  1. **Save** the configuration and **reboot** the device and log in to Windows. |
| Validate Conversion | 1. **Right-click** the **Start** button and select **Disk Management**. 2. **Right-click** on **Disk 0** and select **Properties**. 3. In the **Properties** window, go to the **Volumes** tab. 4. Validate that the **Partition style** is configured as **GUID Partition Table (GPT)**. 5. **Right-click** the **Start** button and select **Run**. 6. Enter **msinfo32** then click **OK**. 7. In the **System Information** window, under **System Summary**, confirm that the **BIOS Mode** item has the **UEFI** value and **Secure Boot State** item has the **On** value. |

### Credential Guard

In this lab, you will activate Credential Guard.

Credential Guard provides an additional layer for protecting secrets, specifically domain user credentials by storing them in a container, secured by the Virtual Secure Mode (VSM), based on Virtualization Based Security (VBS).

These types of containers are separated both from the kernel and the user mode, therefore increasing the difficulty for an attacker, even after compromising the system to steal the credentials directly from Local Security Authority Subsystem (LSASS), for example.

Before working on this lab, you must have:

* A Physical Computer with a Trusted Platform Module (TPM) chip (2.0 recommended), a CPU with VT-x and VT-d capabilities.
* Windows 10 Enterprise running on the Host.
* Local Administrator Account.
* It is recommended that you use a Host for testing purposes. Please do not use your personal machines. Also, the Host must not be domain joined into your company domain, so that there is no compliance or configuration/support issues.

#### Check Credential Guard Requirements

In this exercise, you will:

* Check if the requirements for Credential Guard are fulfilled.
* Manually activate Credential Guard and its dependencies.

| Task | Detailed Steps |
| --- | --- |
| **Complete this activity on the Reference Device provided by the Customer or CLIENT 1-4.** | |
| System Verification | 1. Log in as **.\Administrator or the Local Administrator Account** and open **MSINFO32.EXE** (elevated) and check if:  * BIOS Mode = UEFI * Secure Boot State = On * Hyper-V – Second Level Address Translation Extensions = Yes * Hyper-V – Virtualization Enabled in Firmware = Yes * Hyper-V – Data Execution Protection = Yes  1. If any of the above values are not enabled, then boot into your BIOS/UEFI and activate them. 2. Note that if UEFI is in CSM (compatibility) mode, changing it to UEFI Native will require the partition layout to be GPT instead of MBR (requires formatting the hard drive). |
| TPM Verification | 1. Open **TPM.MSC** and make sure that the TPM is turned on. 2. If TPM is turned off/not visible, make sure that it exists physically and it is enabled in BIOS/UEFI. 3. If the TPM is turned on but not initialized:    1. Create the TPM owner password using **Automatically create the password** option.    2. In the **Save your TPM owner password**, click **Save the password** and select a location to save the password, and then click **Save** (file is saved as computer\_name.tpm).    3. Click **Initialize**.    4. After this, the TPM should be ready for use.   **Note**: The recommended version of TPM is 2.0. Windows might refuse to activate Credential Guard if the computer contains an older TPM version/revision. |
| Enable Required Features | 1. Go to **Control Panel > Programs >** **Turn Windows features on or off**. 2. Check **Hyper-V** and all **sub-options** within it.   **Note:** On a VM, the Hyper-V Hypervisor option might be unselected and greyed out if the host’s processor does not have the required virtualization capabilities.   1. Click **OK**. 2. Restart the computer by clicking **Restart now**.   **Note**: **Hyper-V** supplies the virtualization core. |

#### Cloud Management

Follow the following sections for managing Credential Guard using Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Groups for use with Credential Guard Lab | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values:   GROUP TYPE: **Security**  GROUP NAME: **CredGuardDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**  7. Click **Select | Create**. |
| Creating an Intune Credential Guard Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click on “**+ Create profile**”. 10. For **Platform**, select **Windows 10 and later**. 11. For **Profile**, select **Custom** and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**. |
|  | Name: **Cred Guard Demo**  Description: **Cred Guard Demo**   1. Under the **Configuration settings** tab, Select “**Add**” to add a OMA-URI Setting. 2. Fill out the form and click **Add**:   Name: **Enable VBS**  Description: **Enable VBS**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/EnableVirtualizationBasedSecurity**  Date type: **Integer**  Value: **1**   1. Click **Add** again and fill out the form and click **Add**:   Name: **Enable Configure LsaCfgFlags**  Description: **Enable Configure LsaCfgFlags**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags**  Date type: **Integer**  Value: **1**   1. Click **Add** again and fill out the form and click **Add**:   Name: **Enable Configure Require Platform Security Features**  Description: **Enable Configure Require Platform Security Features**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/RequirePlatformSecurityFeatures**  Date type: **Integer**  Value: **1**   1. Select **Next**. 2. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **CredGuardDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + Create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Verify the Policy has been Applied and Working | 1. Log in to a machine as:   **TU2@<AzureDomainName>.onmicrosoft.com** (You might have to enable MFA for this user on this machine).   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. 9. **Reboot** the machine. 10. Log back in using the same credentials. 11. Click **Start**. 12. Type and click “**System Information**”. 13. Verify that “**Virtualization-based security is running**”.   **Note:** After the first boot it could be “**Enabled but not running**”.   1. **Reboot** the machine again. 2. Click **Start**. 3. Type and click “**System Information**”. 4. Verify that “**Virtualization-based Security is running**”.   **Note:** It can take up to 3 or more reboots and syncing to see that it is running. |

#### On-premises method

Follow the following sections for managing Credential Guard through on-premises management tools.

Configure VBS and Credential Guard

Now that the required features and components are in place, activate the Virtualization Based Security and Credential Guard.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| System Configuration | 1. Log in as **.\Administrator or the Local Administrator Account** and open **gpedit.msc** and accept the UAC prompt if required. 2. Go to **Computer Configuration > Administrative Templates > System >** **Device Guard**. 3. Edit the **Turn On Virtualization Based Security** policy by selecting **Enabled**. 4. Select **Secure Boot** in the **Select Platform Security Level**. 5. Select **Enabled with UEFI lock** in the **Credential Guard Configuration**. 6. Click **Apply** and **OK**. 7. Restart the computer and check “**System Information**” and verify that “**Virtualization-based Security is running**”. |

Troubleshoot Credential Guard

After enabling all of the above features and settings, make sure that no errors were logged and all the components are properly configured.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Logging | 1. Device Guard policies are logged in Event Viewer at **Applications and Services Logs > Microsoft > Windows > DeviceGuard >** **Operational**. 2. An **event ID 7000** should be logged, which contains the selected settings within the policy (when successfully applied). |
| MSInfo32 | 1. Open **MSINFO32.EXE** (elevated) and confirm that the options are defined as in the following screenshot. |
| Registry | 1. Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard**. 2. Verify if **EnableVirtualizationBasedSecurity** is set to **1**. 3. Verify if **RequirePlatformSecurityFeatures** is set to **1** (Secure Boot). 4. Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. 5. Verify if the **LsaCfgFlags** is set to **1**. |
| Process | 1. Open **Task Manager**. 2. Verify the presence of **Lsalso.exe**. |

### Windows Defender Application Guard

Designed for Windows 10 and Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted.

If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V-enabled container, which is separate from the host operating system. This container isolation means that if the untrusted site turns out to be malicious, the host PC is protected, and the attacker can't get to your enterprise data.

**Note:** Windows Defender Application Guard can only be enabled if the Hardware Requirements are met as stated in <https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-application-guard/reqs-wd-app-guard>

**Note:** The Logical Processors and Memory on VMs can be increased from Hyper-V Manager. To know if your Hyper-V Host’s or Physical Machine’s Processor supports SLAT or not, download and extract CoreInfo from <https://docs.microsoft.com/en-us/sysinternals/downloads/coreinfo> and run **coreinfo.exe –v**. If it does not support, you will see a dash else you will see an asterisk. The Virtualization Extensions for VBS can be enabled from BIOS or UEFI.



#### Cloud Management

Follow the following sections for managing Windows Defender Application Guard using Intune.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create Groups for use with WD Application Guard Demo | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDAGDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**  7. Click **Create**. |
| Creating an Intune WDAG Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click on “**+ Create profile**”. 10. Under **Platform**, select **Windows 10 and later**. 11. Under **Profile**, select **Endpoint protection** and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**:   Name: **WDAG Demo**  Description: **WDAG Demo**   1. Under the **Configuration settings** tab, enter the following and click **Next**:   Expand **Microsoft Defender Application Guard**  Application Guard: **Enabled for Edge**  Clipboard behavior: **Block copy and paste between PC and browser**  External content on enterprise sites: **Not configured**  Print from virtual browser: **Allow**  Printing type(s): **PDF**  Collect logs: **Not configured**  Retain user-generated browser data: **Not configured**  Graphics acceleration: **Not configured**  Download files to host file system: **Not configured**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **WDAGDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above).** | |
| Verify the Policy has been Applied and Working | 1. Log in to a machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. Reboot the machine once. 9. Launch **Edge**. 10. Click **New Application Guard window** from the menu. 11. A new window should appear.   **Note:** Notice that in the upper left-hand corner of the window you should see Application Guard and a thin orange line at the top of the windows. This indicates you are running in Application mode.  A screenshot of a cell phone  Description automatically generated   1. Enter the URL **www.bing.com**. 2. Create a new tab. 3. Copy the URL [www.bing.com](http://www.bing.com) to the new tab.   **Note:** Notice that you can do this because it is inside of Application Guard.   1. Open **IE**. 2. Try to copy the URL from WDAG Edge windows to IE.   **Note:** Notice that you cannot copy. This is because WDAG is configured to not allow copy and paste with the OS.   1. Enter the URL of **www.msn.com** in IE. 2. Copy this URL from IE and try and paste it in WDAG Edge window.   **Note:** Notice that you cannot copy. This is because WDAG is configured to not allow copying from the OS to the WDAG Edge windows. |

#### On-premises method

Follow the following sections for managing Windows Defender Application Guard using on-premises management tools.

Prerequisites

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above).** | |
| Install the Feature | 1. Open the **Control Panel**, click **Programs,** and then click **Turn Windows features on or off**. 2. Select the checkbox next to **Windows Defender Application Guard** and then click **OK**. 3. Restart the device. |

Configure Group Policy Settings

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Turn On Windows Defender Application Guard | 1. In the **Group Policy Management** Console, edit the **Default Domain Policy** by going to **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Application Guard**. 2. Double-click **Turn on Windows Defender Application Guard in Enterprise Mode**. 3. Select **Enabled** and click **Apply** and **OK**. |
| Set Up Network Isolation | 1. Go to the **Computer Configuration\Policies\Administrative Templates\Network\Network Isolation\Enterprise resource domains hosted in the cloud**. 2. Select **Enabled** and type **.microsoft.com** into the **Enterprise cloud resources** box. Click **Apply** and **OK**. 3. Go to the **Computer Configuration\Policies\Administrative Templates\Network\Network Isolation\Domains categorized as both work and personal** setting. 4. Select **Enabled** and type **bing.com** into the **Neutral resources** box. Click **Apply** and **OK**. |

Validate Windows Defender Application Guard

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above).** | |
| Test Application Guard | 1. Update the group policies by running **gpupdate /force** from the elevated command prompt. Accept the UAC prompt if required. 2. Start Microsoft Edge and type [www.microsoft.com](http://www.microsoft.com) 3. After you submit the URL, Application Guard determines the URL is trusted because it uses the domain you’ve marked as trusted and shows the site directly on the host PC instead of in Application Guard. 4. In the same Microsoft Edge browser, type any URL that isn’t part of your trusted or neutral site lists, example [www.msn.com](http://www.msn.com) 5. After you submit the URL, Application Guard determines the URL is untrusted and redirects the request to the hardware-isolated environment. |

### Windows Defender Exploit Guard

Windows Defender Exploit Guard (Windows Defender EG) is a new set of host intrusion prevention capabilities for Windows 10, allowing you to manage and reduce the attack surface of apps used by your employees.

There are four features in Windows Defender EG:

* Exploit protection can apply exploit mitigation techniques to apps your organization uses, both individually and to all apps.
* Attack surface reduction rules can reduce the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script- and mail-based malware.
* Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Edge to cover network traffic and connectivity on your organization's devices.
* Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware.

#### Cloud Management

Follow the following sections for managing Windows Defender Exploit Guard through cloud management tools.

Exploit Guard Controlled Folders

In this section, we are going to create a group that will be used to assign users an Exploit Guard controlled folder policy. In addition we will configure the policy and test that it works.

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | | | |
| Create Groups | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **ExploitDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. | | |
| Configure Windows Defender Exploit Guard | | 1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Under Manage Select “**Device configuration**”. 5. Under Manage Select “**Profiles**”. 6. Select “**Create profile**”. 7. Under **Platform**, select **Windows 10 and later**. 8. Under **Profile**, select **Windows 10 and later** and click **Create**. 9. Under the **Basics** tab, enter the following information and click **Next**:   Name: **Exploit Protection Demo**   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Expand **Microsoft Defender Exploit Guard** |
|  | | Expand **Controlled folder access**  Folder protection: **Enable**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **ExploitDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.** | | |
| Verify Configuration is Applied | | 1. Log in to the virtual machine as   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Open up **Notepad.exe**. 9. Create a simple document. 10. Save it to “**Documents**”.   **Note:** Notice you cannot save to Documents because this is a protected folder. You will get a “**File not found**” message.   1. Press **OK**. |

#### On-premises method

Follow the following sections for managing Windows Defender Exploit Guard through on-premises management tools.

Exploit Protection

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Configure Program-Level Mitigations | 1. Open the **Windows Security** by clicking the shield icon in the taskbar or searching the start menu for **Security**. 2. Click the **App & browser control** tile (or the app icon on the left menu bar) and then the **Exploit protection settings** at the bottom of the screen. 3. Go to the **Program settings** section and click **Add program to customize**. 4. Click on **Add by program name** and type **notepad.exe**. Click **Add**. 5. On the next window, scroll down and on **Disable Win32k system calls**, select **Override system settings** and choose **On**. 6. You will be notified if you need to restart the process or app, or if you need to restart Windows. Click **Apply** and accept the UAC prompt if required. 7. Try to open **notepad.exe**. Notice the error message. Click **OK**. |
| Create and Export a Configuration File | 1. Open the **Windows Security** by clicking the shield icon in the taskbar or searching the start menu for **Security**. 2. Click the **App & browser control** tile (or the app icon on the left menu bar) and then the **Exploit protection settings** at the bottom of the screen. 3. At the bottom of the **Exploit protection** section, click **Export settings** and then save the configuration file under **Documents**. 4. Copy the file to **DC1** in a shared folder with full permissions. |
| **Complete these steps on the DC1 virtual machine.** | |
| Distribute the Configuration File with Group Policy | 1. On your Group Policy management machine, open the **Group Policy Management Console**, right-click the **Group Policy Objects** and create a new GPO **WDEG**. 2. Right-click the new Group Policy **WDEG** and click **Edit**. 3. In the **Group Policy Management Editor** go to **Computer Configuration**. 4. Click **Policies** then **Administrative Templates**. 5. Expand the tree to **Windows Components > Windows Defender Exploit Guard > Exploit Protection**. 6. Double-click the **Use a common set of exploit protection settings** setting and set the option to **Enabled**. 7. In the **Options** section, enter the location and filename of the Exploit Protection Configuration File that you saved from the previous section in a UNC format including the name of the file and it’s extension and click **Apply | OK**. |

Attack Surface Reduction

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Distribute the Configuration File with Group Policy | 1. On your Group Policy management machine, open the **Group Policy Management Console**, and right-click the Group Policy Object **WDEG**. 2. Click **Edit**. 3. In the **Group Policy Management Editor** go to **Computer Configuration**. 4. Click **Policies** then **Administrative Templates**. 5. Expand the tree to **Windows Components > Windows Defender Antivirus > Windows Defender Exploit Guard > Attack Surface Reduction**. 6. Double-click the **Configure Attack Surface Reduction rules** setting and set the option to **Enabled**.   Click **Show...** and enter the following rule ID in **Value name:**  **D3E037E1-3EB8-44C8-A917-57927947596D**   1. Set the **Value** to **1** and click **OK**. Click **Apply | OK**. 2. Link the GPO **WDEG** to the root domain.   **Note:** The above rule will block JavaScript or VBScript from launching downloaded executable content as well as block notepad.exe to launch. Do run a **gpupdate /force** on the **CLIENT2** VM. |

### Windows Defender Application Control

With thousands of new malicious files created every day, using traditional methods like antivirus solutions—signature-based detection to fight against malware—provides an inadequate defense against new attacks.

In most organizations, information is the most valuable asset, and ensuring that only approved users have access to that information is imperative. However, when a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organization if a user knowingly or unknowingly runs malicious software.

Application control can help mitigate these types of security threats by restricting the applications that users are allowed to run and the code that runs in the System Core (kernel). Application control policies can also block unsigned scripts and MSIs, and restrict Windows PowerShell to run in [Constrained Language Mode](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes).

Application control is a crucial line of defense for protecting enterprises given today’s threat landscape, and it has an inherent advantage over traditional antivirus solutions. Specifically, application control moves away from an application trust model where all applications are assumed trustworthy to one where applications must earn trust in order to run.



#### Cloud Management

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | | | |
| Create Groups for use with WDAC Demo | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDACDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. | | |
| Configuring WDAC with Intune | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Click on “**Device configuration**”. 5. Click on “**Profiles**”. 6. Click on “**+ Create profile**”. 7. Under **Platform**, select **Windows 10 and later**. 8. Under **Profile**, select **Endpoint protection** and click **Create**. 9. Under the **Basics** tab, enter the following information and click **Next**: | | |
|  | Name: **WDAC Demo**  Description: **WDAC Demo**   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Expand **Microsoft Defender Application Control**  Application control code integrity policies: **Enforce**  Trust apps with good reputation: **Enable**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **WDACDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. | | |
| **Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support**  **nested virtualization.** | | | |
| Verify Configuration is Applied | 1. Log in to the virtual machine as   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. In **DC1**, download **camstudio** from <http://camstudio.org> to **C:\Packages**. 9. Back in **CLIENT3**, copy **camstudio** from **\\DC1\C$\Packages** to the **Desktop**. 10. Try and install the application **camstudio**. 11. The app will be blocked by WDAC when you try and install it. | | |

#### On-premises method

In this section, you will learn how to Configure and Deploy Code Integrity Policies and Enable Device Guard in an enterprise.

**Note:** Ignore any errors or warnings from the PowerShell commands below.

Prerequisites

Perform the following tasks before proceeding to the succeeding sections.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Download VLC Media Player | 1. Open Internet Explorer and browse to the URL below.   <http://www.videolan.org/vlc/>   1. Click **Download VLC** and save **vlc-3.0.10-win64.exe** to **C:\Packages**. |
| Download CamStudio (Ignore if already downloaded from the previous lab) | 1. Open Internet Explorer and browse to the URL below.   <http://camstudio.org/>   1. Click **Download** and save **camstudio.exe** to **C:\Packages**. |

Create CI Policy from a Golden System

In this activity, you will go through the steps in creating your first Code Integrity (CI) policy from a “Golden” system.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Open PowerShell | 1. Logon as a Domain Administrator (**corp\labadmin**) and from the Start Menu, start an elevated instance of PowerShell. |
| Create Shadow Copy of System Drive | 1. From the PowerShell window, run the following commands:   **$s1 = (gwmi -List Win32\_ShadowCopy).Create("C:\", "ClientAccessible")**  **$s2 = gwmi Win32\_ShadowCopy | ? { $\_.ID -eq $s1.ShadowID }**  **$d = $s2.DeviceObject + "\"**  **cmd /c mklink /d C:\scpy "$d"** |
| Generate a New Policy from Scan | 1. From the PowerShell window, run the following commands:   **New-CIPolicy -level PcaCertificate -filepath C:\PoCPolicy.xml –scanpath C:\scpy –u**  **Note:** It may take around 20-30 minutes and during the process a base policy will already be created and also if required, increase the memory of the virtual machine for this process to run efficiently. Ignore any errors received after command execution completes. |
| Explore Policy Configuration | 1. Save the file **PoCPolicy.xml** to a network location, example: **\\DC1\C$**. 2. Open the file and review the content without making changes. Open the file **C:\PoCPolicy.xml** with IE. 3. Close the file. |

Configurable Code Integrity – Audit Mode

In this activity, you will create a CI policy and deploy it in audit mode.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Convert from XML to Binary File | 1. From the PowerShell window, run the following commands:   **ConvertFrom-CIPolicy C:\PoCPolicy.xml C:\PoCPolicy.bin** |
| Install Complied Policy | 1. From the PowerShell window, run the following commands:   **cp C:\PoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b**   1. Restart **CLIENT1** and re-log in with the same credentials. |
| Verify Audit Logs | 1. Launch the installation package for VLC located at **\\DC1\C$\Packages\vlc-3.0.10-win64.exe** and install the package. The installation will be successful at this point. 2. Right-click on the **Start** button and click **Run**. 3. Enter **eventvwr.msc** and click **OK**. 4. In the Event Viewer MMC, browse to **Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows >** **CodeIntegrity >** **Operational**. 5. Browse through the log files especially **Event ID 3076**. |

Creating CI Policy from Audit Logs

In this activity, you will go through the steps in creating a Code Integrity (CI) policy from audit log events.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Create a CI Policy from Audit Logs | 1. From the Start Menu, start an elevated instance of PowerShell. 2. From the PowerShell window, run the following commands:   **New-CIPolicy -l PcaCertificate -f C:\AuditPoCPolicy.xml –a –u**  **Note**: Ignore any errors received after command execution completes.   1. Open the file **C:\AuditPoCPolicy.xml** with IE. 2. Close the file. |
| Merge Golden Policy with Policy from Audit Logs | 1. From the PowerShell window, run the following commands:   **Merge-CIPolicy –OutputFilePath C:\MergedPoCPolicy.xml –PolicyPaths C:\AuditPoCPolicy.xml,C:\PoCPolicy.xml**   1. Open the file **C:\MergedPoCPolicy.xml** with IE. 2. Close the file. |

Configurable Code Integrity – Enforce Mode

In this activity, you will deploy and enforce a CI policy to lock down the system.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Disable Audit Mode | 1. From the PowerShell window, run the following commands:   **Set-RuleOption –option 3 -delete –FilePath C:\MergedPoCPolicy.xml**   1. Open the file **C:\MergedPoCPolicy.xml** with IE. 2. Close the file. |
| Convert from XML to Binary File | 1. From the PowerShell window, run the following commands:   **ConvertFrom-CIPolicy C:\MergedPoCPolicy.xml C:\MergedPoCPolicy.bin** |
| Install Compiled Policy | 1. From the PowerShell window, run the following commands:   **cp C:\MergedPoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b**   1. Restart **CLIENT1** and re-log in with the same credentials. |
| Install or Launch Your Application(s) | 1. Launch the installation package for CamStudio or VLC located at **\\DC1\C$\Packages\camstudio.exe** or **\\DC1\C$\Packages\vlc-3.0.10-win64.exe**. The application should not launch at this stage and throw errors, which means it is blocked by code integrity. |
| Verify Audit Logs | 1. Right-click on the **Start** button and click **Run**. 2. Enter **eventvwr.msc** and click **OK**. 3. In the Event Viewer MMC, browse to **Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows >** **CodeIntegrity >** **Operational**. 4. Browse through the log files especially **Event ID 3077**. |

Configure Group Policies

In this activity, you will learn how to configure and deploy group policies to enforce the configuration.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 and the CLIENT2 virtual machines.** | |
| Create Device Guard GPO | 1. Create a folder in the **C:** drive by the name **CodeIntegrity** and in this folder, copy the **SIPolicy.p7b** file created in the previous task from the **CLIENT1** VM. The path of this file in the **CLIENT1** VM is **C:\Windows\System32\CodeIntegrity**. 2. Navigate to **C:\CodeIntegrity**, right-click **CodeIntegrity** folder and click **Properties**. 3. Click the **Sharing** tab and click **Advanced Sharing…** 4. Check the box next to **Share this folder** and click **Permissions**. 5. Ensure **Everyone** is in the list and has been granted **Full Control**. Click **Apply** and click **OK** two times. 6. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 7. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows. 8. Now navigate to **C:\CodeIntegrity\SIPolicy.p7b** that has been copied and right-click on the file and click **Properties**. 9. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 10. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows.   **Note**: Check to see that everyone has been granted Full Control permissions.   1. Back in the **DC1** VM, in the Active Directory Users and Computers, create an OU called **Devices** (if not already created from the previous labs) and move the **CLIENT2** VM to the **Devices** OU from the default **Computers** container. 2. Open the **Group Policy Management Console**. 3. Right-click on **Group Policy Management > Forest: corp.contoso.com > Domains > corp.contoso.com >** **Group Policy Objects** and select **New**. 4. Under Name, enter **Device Guard Policies** and then click **OK**. 5. Right-click **Devices** OU, click **Link an Existing GPO**… 6. Select **Device Guard Policies** and click **OK**. |
| Deploy Code Integrity Policy and Enable VBS for KCMI | 1. Right-click **Device Guard Policies** and select **Edit**. 2. Browse to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**. 3. Double-click on **Deploy Windows Defender Application Control**. 4. Select **Enabled**. 5. Under Code Integrity Policy file path, enter **\\DC1\CodeIntegrity\SIPolicy.p7b**. 6. Click **Apply** and then **OK**. 7. Double-click on **Turn On Virtualization Based Security**. 8. Select **Enabled**. 9. Under Select Platform Security Level, select **Secure Boot and DMA Protection**. 10. Under Virtualization based Protection of Code Integrity, select **Enabled with UEFI lock**. 11. Click **Apply** and then **OK**. |
| Attempt to Run New Applications that have not installed on the System | 1. Now on the **CLIENT2** VM, run a **gpupdate /force**. 2. Restart **CLIENT2** and re-log in with the same credentials. 3. Verify that any new application installation or new executable is blocked by the Code Integrity Policy, Example: **CamStudio** or **VLC**. The CamStudio package is located at **\\DC1\C$\Packages\camstudio.exe** and the VLC package is located at **\\DC1\C$\Packages\vlc-3.0.10-win64.exe**.   **Note:** In case the CamStudio package is missing in **\\DC1\C$\Packages\camstudio.exe**, re-download it by following **Steps 3-4** of **Section 8.8.2.1**.  **Note:** Before executing any labs after the Code Integrity Lab in which the **CLIENT1** and **CLIENT2** VMs are going to be used, ensure that they and any other machines have been moved to the default **Computers** container from the **Devices** OU. Also ensure that there are no other Client VMs in that OU and have been moved to the default **Computers** container. Then in both the VMs, delete the **SIPolicy.p7b** file from **c:\Windows\System32\CodeIntegrity**. Run a **gpupdate /force** and reboot both the VMs. This is to ensure that no activity is blocked by Code Integrity. |

### Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a security service that enables enterprise customers to detect, investigate, and respond to advanced threats on their networks.

Windows Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

* **Endpoint behavioral sensors**: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system (for example, process, registry, file, and network communications) and sends this sensor data to your private, isolated, cloud instance of Windows Defender ATP.
* **Cloud security analytics**: Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem (such as the Microsoft Malicious Software Removal Tool, enterprise cloud products (such as Microsoft 365), and online assets (such as Bing and SmartScreen URL reputation), behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
* **Threat intelligence**: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Windows Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

In this section, you will learn how to configure and use Windows Defender ATP to detect and respond to threats.

**Note:** This lab can only be performed if the customer has already registered and approved for the Microsoft WDATP Preview/Trial program (Section 3.2.3).

#### Onboarding Windows 10 Device

In this activity, you onboard your first Windows 10 client to Windows Defender Advanced Threat Protection.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Download the Onboarding Package | 1. Log in to the device. 2. Navigate to [**https://securitycenter.windows.com/**](https://securitycenter.windows.com/) 3. **Sign in** to the portal with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. On the Get started page, click **Next**. 5. On the Set up preferences page, select the appropriate data storage location. 6. Select the appropriate data retention policy. 7. Select your appropriate organization size. 8. Keep the preview features on and then click **Next**. 9. Click **Continue** to create a cloud instance. It will start creating your Windows Defender ATP cloud instance. 10. On the Onboard a machine page, under **Deployment method** dropdown, select **Local Script (for up to 10 machines)** and click **Download package**. 11. Click **Save as** and **Save** the package to **C:\**. 12. Click **Start using Microsoft Defender ATP** and click **Proceed anyway**. |
| Execute the Onboarding Package | 1. Navigate to **C:\**, right-click the package and click **Extract All…** 2. Click **Extract**. 3. Navigate to the extracted package, right-click on the script file and click **Edit**.   **Note**: Note the registry paths we are writing to. Note the log and the Event ID we are creating in case of successful events using eventcreate.   1. Close notepad. 2. Right-click the script file and click **Run as administrator**. Press **Y** to confirm and continue. **Press any key to continue**. 3. After 5-10 minutes the machine will be onboarded. 4. In the **Microsoft Defender Security Center**, on the left navigation pane, click **Settings**. Scroll down and then under **Machine management**, click **Onboarding**. Scroll down and then under **Run a detection** test, copy the command snippet and run it in an elevated command prompt window. Once successful, the detection test will be marked as **Completed**. |
| Configure the Sample Collection Setting | 1. Click the **Start** menu and type **regedit**, right-click and choose **Run as administrator**. 2. Locate the following registry path: **HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection**. 3. Create a **DWORD** value **AllowSampleCollection** and set it to **1**.   **Note**: The machine will file sample collection through the portal for deeper investigation. No samples are collected automatically as this is done by the administrator. |
| Verify the Deployment Success | 1. Check the SENSE service is running, by opening the Command Prompt and running: **sc query sense**. The **STATE** should be **4** and should be **RUNNING**. 2. Open the **Event Viewer (Local) > Windows Logs > Application** log and locate the **Event ID 20** from the source **WDATPOnboarding**. 3. Open the **Event Viewer (Local) > Application and Services Logs > Microsoft > Windows > SENSE >** **Operational** log. Check for the **Event ID 13** to make sure that the SENSE service has a normal operating process. Connection frequency may vary depending on factors like battery state. 4. Go to [**https://securitycenter.windows.com/**](https://securitycenter.windows.com/)portal, then choose **Machines list**, on the right locate your machine on the list, its **Health State** should be **Active**. |
| Install Office (If Not Installed) | 1. Go to [**https://portal.office.com**](https://portal.office.com)and **Sign in** as **TU2@<AzureDomainName>.onmicrosoft.com** 2. Click **Install Office 365 > Office 365 apps**. 3. Click **Run**. |

#### Perform Simulation

In this activity, you will go step-by-step through a typical attack sequence that you will run yourself.

**Note:** The setup guide also contains instructions and links for the attack demo.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Follow the Demo Attack Simulation Guidance | 1. Click the link to download and open the **RS4\_WinATP-Intro-Invoice.docm** word document from the setup guide or <https://securitycenter.windows.com/tutorials> **(Scenario 1 - Get simulation file)**. 2. Since the device has Microsoft 365 installed, therefore click **Yes** and **OK** on the Microsoft 365 security prompts if required. 3. Enter the password to open the word document and click **OK**. The password is provided in the setup guide. 4. Click **Enable Editing** and **Enable Content** on the opened word document. 5. Click **OK** on the prompt. 6. A Backdoor will run in a command window. **Press any key to close**. 7. You will now be able to see that an Active alert has been reported to the Windows Defender Advanced Threat Protection by the device. Navigate through the portal for further details on the attack and ways to remediate. |

### Endpoint Security - Security Baselines

Use Intune's security baselines to help you secure and protect your users and devices. Security baselines are pre-configured groups of Windows settings that help you apply a known group of settings and default values that are recommended by the relevant security teams. When you create a security baseline profile in Intune, you're creating a template that consists of multiple *device configuration profiles*.

You deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10 or later. For example, the *MDM Security Baseline* automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, automatically disables basic authentication, and more. When a default value doesn't work for your environment, customize the baseline to apply the settings you need.

Separate baseline types can include the same settings but use different default values for those settings. It's important to understand the defaults in the baselines you choose to use, and to then modify each baseline to fit your organizational needs.

**Note:** Microsoft doesn't recommend using preview versions of security baselines in a production environment. The settings in a preview baseline might change over the course of the preview.

Security baselines can help you to have an end-to-end secure workflow when working with Microsoft 365. Some of the benefits include:

* A security baseline includes the best practices and recommendations on settings that impact security. Intune partners with the same Windows security team that creates group policy security baselines. These recommendations are based on guidance and extensive experience.
* If you're new to Intune, and not sure where to start, then security baselines gives you an advantage. You can quickly create and deploy a secure profile, knowing that you're helping protect your organization's resources and data.
* If you currently use group policy, migrating to Intune for management is much easier with these baselines. These baselines are natively built in to Intune, and include a modern management experience.

[Windows security baselines](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines) is a great resource to learn more about this feature. [Mobile device management](https://docs.microsoft.com/en-us/windows/client-management/mdm/) (MDM) is a great resource about MDM, and what you can do on Windows devices.

For more information, refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

For a full list of Windows MDM security baseline settings for intune, specially the latest baseline in Intune (May 2019), refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-mdm-all?pivots=mdm-may-2019>

**Note:** In order to test some settings of the Security Baseline Profile on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Device Configuration Profiles from the previous labs.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy a Security Baseline Profile | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Endpoint security** > **Security baselines** to view the list of available baselines. 3. Select the baseline you'd like to use, example: **Windows 10 Security Baselines** and then select **+ Create profile**. 4. On the **Basics** tab, specify the following properties:  * **Name**: Enter a name for your security baselines profile. * **Description**: Enter some text that describes what this baseline does. The description is for you to enter any text you want. It's optional, but recommended.   Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab.   1. On the **Configuration settings** tab, view the groups of **Settings** that are available in the baseline you selected. You can expand a group to view the settings in that group, and the default values for those settings in the baseline. For a full list of Windows MDM security baseline settings for intune, specially the latest baseline in Intune (May 2019), refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-mdm-all?pivots=mdm-may-2019>. To find specific settings:  * Select a group to expand and review the available settings. * Use the *Search* bar and specify keywords that filter the view to display only those groups that contain your search criteria.   Each setting in a baseline has a default configuration for that baseline version. Reconfigure the default settings to meet your business needs. Different baselines might contain the same setting, and use different default values for the setting, depending on the intent of the baseline.  Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab.   1. On the **Scope tags** tab, select **+ Select scope tags** to open the *Select tags* pane to assign scope tags to the profile. Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab. 2. On the **Assignments** tab, select **+ Select groups to include** and then assign the baseline to one or more groups. Use **+ Select groups to exclude** to fine-tune the assignment. Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab. 3. When you're ready to deploy the baseline, advance to the **Review + create** tab and review the details for the baseline. Select **Create** to save and deploy the profile.   As soon as you create the profile, it's pushed to the assigned group and might apply immediately.  **Note:** If you save a profile without first assigning it to groups, you can later edit the profile to do so.   1. After you create a profile, edit it by going to **Endpoint security** > **Security baselines**, select the baseline type that you configured, example: **Windows 10 Security Baselines** and then select **Profiles**. Select the profile from the list of available profiles, and then select **Properties**. You can edit settings from all the available configuration tabs, and select **Review + save** to commit your changes. |

### Endpoint Security – Device Compliance

Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version. If the device isn't compliant, you can then block access to data and resources using [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access).

You can also take actions for non-compliance, such as sending a notification email to the user. For an overview of what compliance policies do, and how they're used, see [get started with device compliance](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started).

**Note:** In order to test some settings of the Device Compliance Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Device Compliance Policies from the previous labs.

**Note:** For platforms other than Windows 10, they must be available with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Device Compliance Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Devices** > **Compliance policies** > **Policies** > **+ Create Policy**. 3. Select a **Platform** for this policy from the following options:  * *Android device administrator* * *Android Enterprise* * *iOS/iPadOS* * *macOS* * *Windows Phone 8.1* * *Windows 8.1 and later* * *Windows 10 and later*   For *Android Enterprise*, you also select a **Policy type**:   * *Android device owner compliance policy* * *Android work profile compliance policy*   Then, select **Create** to open the **Create policy** configuration window.   1. On the **Basics** tab, specify a **Name** that helps you identify them later. You can also choose to specify a **Description**. Click **Next**. 2. On the **Compliance settings** tab, expand the available categories, and configure settings for your policy. Click **Next**. The following articles describe the settings for each platform:  * [Android device administrator](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android) * [Android Enterprise](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work) * [iOS/iPadOS](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios) * [macOS](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-mac-os) * [Windows Phone 8.1, Windows 8.1 and later](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows-8-1) * [Windows 10 and later](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows)  1. On the **Locations** tab, you can force compliance based on the location of the device. Choose from existing locations. If you don't have an available location yet, see [Use Locations (network fence)](https://docs.microsoft.com/en-us/mem/intune/protect/use-network-locations) for guidance. Click **Next**.   **Note:** **Locations** are available only for the *Android device administrator* platform.   1. On the **Actions for noncompliance** tab, specify a sequence of actions to apply automatically to devices that don't meet this compliance policy and click **Next**.   You can add multiple actions and configure schedules and additional details for some actions. For example, you might change the schedule of the default action *Mark device noncompliant* to occur after one day. You can then add an action to send an email to the user when the device isn't compliant to warn them of that status. You can also add actions that lock or retire devices that remain noncompliant.  For information about the actions you can configure, see [Add actions for noncompliant devices](https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance), including how to create notification emails to send to your users.  Another example includes the use of Locations where you add at least one location to a compliance policy. In this case, the default action for noncompliance applies when you select at least one location. If the device isn't connected to any of the selected locations, it's considered not compliant. You can configure the schedule to give your users a grace period, such as one day.   1. On the **Scope tags** tab, select tags to help filter policies to specific groups, such as **US-NC IT Team** or **JohnGlenn\_ITDepartment**. After you add the settings, you can also add a scope tag to your compliance policies. Click **Next**.   For information on using scope tags, see [Use scope tags to filter policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags).   1. On the **Assignments** tab, assign the policy to your groups and click **Next**.   Select **+ Select groups to include** and then assign the policy to one or more groups. The policy will apply to these groups when you save the policy after the next step.   1. On the **Review + create** tab, review the settings and select **Create** when ready to save the compliance policy.   The users or devices targeted by your policy are evaluated for compliance when they check in with Intune. |

### Endpoint Security – Manage Antivirus, Disk Encryption and Firewall

As a security admin, use the security policies from the *Endpoint security* of Intune to configure device security without the overhead of navigating the larger body and range of settings found in device configuration profiles and security baselines.

Each policy type supports one or more profiles. Profiles are where you configure settings and can group settings for different platforms, or for different areas of focus in the larger policy area.

You'll find these policies under Manage in the **Endpoint security** node of the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431).

For more information, refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy>

**Note:** In order to test some settings of the Device Compliance Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Antivirus, Disk Encryption and Firewall Policies from the previous labs.

**Note:** For platforms other than Windows 10, they must be available with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Antivirus, Disk Encryption and Firewall Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Endpoint security** and then select the type of policy you want to configure, and then select **+ Create Policy**. Choose from the following policy types:  * Antivirus * Disk encryption * Firewall  1. Enter the following properties:  * **Platform**: Choose the platform that you're creating policy for. The available options depend on the policy type you selected: * macOS * Windows 10 and later * **Profile**: Choose from the available profiles for the platform you selected. For information about the profiles, see the dedicated sections below for your chosen policy type: * [Antivirus](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-antivirus-policy) * [Disk encryption](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-disk-encryption-policy) * [Firewall](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-firewall-policy)  1. Select **Create**. 2. On the **Basics** page, enter a name and description for the profile, then choose **Next**. 3. On the **Configuration settings** page, expand each group of settings, and configure the settings you want to manage with this profile. When your done configuring settings, select **Next**. 4. On the **Scope tags** page, choose **+ Select scope tags** to open the *Select tags* pane to assign scope tags to the profile. Select **Next** to continue. 5. On the **Assignments** page, select the groups that will receive this profile. Select **Next**. 6. On the **Review + create** page, when you're done, choose **Create**. The new profile is displayed in the list when you select the policy type for the profile you created. |

### Endpoint Security – Conditional Access

With Intune, enhance Conditional Access in Azure Active Directory by adding mobile device compliance to the access controls. With Intune compliance policy that defines requirements for devices to be compliant, you can use a device's compliance status to either allow or block access to your apps and services. You can do this by creating a Conditional Access policy that uses the setting **Require device to be marked as compliant**.

A Conditional Access policy specifies the app or services you want to protect, the conditions under which the apps or services can be accessed, and the users the policy applies to. Although Conditional Access is an Azure AD premium feature, the Conditional Access node you access from *Intune* is the same node as accessed from *Azure AD*.

**Note:** Before you set up Conditional Access, you'll need to set up Intune device compliance policies to evaluate devices based on whether they meet specific requirements. Refer to **Section 8.11: Endpoint Security – Device Compliance**.

**Note:** In order to test some settings of the Conditional Access Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, start their enrollment fresh for them to receive the Device Compliance Policies and for them to be evaluated by the Conditional Access Policies.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Conditional Access Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Devices** > **Conditional Access** > **Policies** > **+ New policy**. 3. Under **Assignments**, select **Users and groups**. 4. On the **Include** tab, identify the users or groups that this Conditional Access policy applies to. Once you've chosen groups or users to include, use the **Exclude** tab if there are any users, roles, or groups you want to exclude from this policy.  * **All users**: Select this option to apply the policy to all users and groups, including internal and guest users. * **Select users and groups**: Select this option and specify one or more of the following options: * **All guest and external users**: Select this option to include or exclude external guest users (for example, partners, external collaborators) * **Directory roles**: Select one or more Azure AD roles to include or exclude users who are assigned these roles. * **Users and groups**: Select this option to search for and select individual users or groups you want include or exclude.   **Note: Test the policy against a smaller group of users to make sure it works as expected.**   1. Select **Done**. 2. Under **Assignments**, select **Cloud apps or actions**. 3. On the **Include** tab, use available options to identify the apps and services you want to protect with this Conditional Access policy. Then you can use the **Exclude** tab if there are any apps or services you want to exclude from this policy.  * **All cloud apps**: Select this option to apply the policy to all apps.   **Note**: The Microsoft Azure Management app for access to the Azure portal is included in this list. Be sure to use the **Exclude** tab either here or in the **Users and groups** options to make sure you (or the users or groups you designate) will be able to sign in to the Azure portal.   * **Select apps**: Select this option, choose **Select**, and then use the applications list to search for and select the apps or services you want to protect.   When ready, select **Done**.   1. Under **Assignments**, select **Conditions**.  * **Sign-in risk**: Select *Yes* to use Azure AD Identity Protection sign-in risk detection with this policy, and then choose the sign-in risk levels the policy should apply to. * **Device platforms**: On the **Include** tab, identify the device platforms you want to this Conditional Access policy to apply to. Use the **Exclude** tab to exclude platforms from this policy. * **Locations**: On the **Include** tab, specify whether the policy applies to: * Any location * Trusted network locations that are under the control of your IT department * Specific network locations.   Use the **Exclude** tab to exclude network locations from this policy.   * **Client apps**: Select *Yes* to specify if the policy should apply to browser apps, mobile apps, and desktop clients. * **Device state**: The Conditional Access policy will apply to all device states unless you choose Yes and specifically exclude the states Device Hybrid Azure AD joined or Device marked as compliant (or both).   **Note**: If you want to protect both **Modern authentication** clients and **Exchange ActiveSync** clients, create two separate Conditional Access policies, one for each client type. Although Exchange ActiveSync supports modern authentication, the only condition that is supported by Exchange ActiveSync is platform. Other conditions, including multi-factor authentication, are not supported. To effectively protect access to Exchange Online from Exchange ActiveSync, create a Conditional Access policy that specifies the cloud app Microsoft 365 Exchange Online and the client app Exchange ActiveSync with Apply policy only to supported platforms selected.   1. Select **Done**. 2. Under **Access controls**, select **Grant**. Configure what happens based on the conditions you've set up. You can select from the following options:  * **Block access**: The users specified in this policy will be denied access to the apps under the conditions you've specified. * **Grant access**: The users specified in this policy will be granted access, but you can require any of the following further actions: * **Require multi-factor authentication**: The user will need to complete additional security requirements, like a phone call or text. * **Require device to be marked as compliant**: The device must be Intune compliant. If the device is noncompliant, the user will be given the option to enroll the device in Intune. * **Require Hybrid Azure AD joined device**: Devices must be Hybrid Azure AD joined. * **Require approved client app**: The device must use approved client apps. * **For multiple controls**: Select **Require all the selected controls** so that all of the requirements are enforced when a device attempts to access the app.  1. Under **Enable policy**, select **On**. 2. Select **Create**. |

# Prepare Applications

## Readiness Toolkit for Office

The Readiness Toolkit for Office add-ins and VBA can help you identify compatibility issues with your Microsoft Visual Basic for Applications (VBA) macros and add-ins that you use with Office. The Readiness Toolkit includes the Readiness Report Creator, which creates an Excel report with VBA macro compatibility and add-in readiness information to help your organization assess its readiness to move to Microsoft 365 Apps for enterprise.

In this section, we will download and install the Readiness Toolkit for Office add-ins and VBA and then create a Readiness Report on a Windows 7 VM.

**Note: Before starting with this scenario, Install Office from the portal using any test user account (if not already installed).**

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT7 virtual machine.** | |
| Download and Install the Readiness Toolkit for Office add-ins and VBA | 1. Log in to **CLIENT7** as **CORP\LabAdmin** and then open Internet Explorer and browse to <https://www.microsoft.com/en-us/download/details.aspx?id=55983>. 2. Click **Download** and save the file **ReadinessToolkitForOffice** to the desktop. 3. On the desktop, right-click **ReadinessToolkitForOffice** and click **Install**. 4. Click **Run**. 5. On the Welcome to the Readiness Toolkit for Office Add-ins and VBA Setup Wizard screen, click **Next**. 6. On the Select Installation Folder screen. click **Next**. 7. On the License Agreement screen, select **I Agree** and then click **Next**. 8. On the Confirm Installation screen, click **Next**. 9. On the Installation Complete screen, click **Close**. |
| Create a Readiness Report | 1. Open **Word**, **Excel** and **PowerPoint** to generate some data for the report and then save and close them. 2. Click **Start | All Programs** and then click **Readiness Toolkit for Office**. 3. After the Readiness Toolkit for Office is launched, on the Create a readiness report screen, select **Most recently used Office documents and installed add-ins on this computer** and then click **Next**. 4. On the Report settings screen, keep the default as **C:\Users\LabAdmin\Documents** and select **Conceal file names and paths** and also select **Scan all Office documents to detect Silverlight or Flash controls. Report creation will take longer** and then click **Next**. 5. On the Which type of readiness report do you want to create? screen, select **Advanced** and then click **Create**. 6. The report creation will start. 7. Once the report is created, you may click **Open in Excel** to view the report directly or you may click **Open file location** to go to the location and open the report in Excel. 8. Click **Enable Content** and go through the various tabs at the bottom of the report. 9. On the Readiness Toolkit for Office window, click **Close**.   **Note:** For more information, refer to <https://docs.microsoft.com/en-us/deployoffice/use-the-readiness-toolkit-to-assess-application-compatibility-for-office-365-pro>. |

## MSIX Packaging and Conversion of Win32 Applications

The MSIX Packaging Tool is a cross-platform, down-level compliant, enterprise-class installer that enables you to modernize app deployment and distribute LOB apps through the Microsoft Store, Microsoft Store for Business, and other methods. The MSIX Packaging Tool enables you to repackage your existing Win32 applications to the MSIX format.

In this section, you will repackage a Win32 application, example: **XmlNotepad.msi** into a MSIX format.

For more information on the MSIX Packaging Tool, refer to <https://docs.microsoft.com/en-us/windows/msix/mpt-overview>

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT4 virtual machine.** | |
| Download and Install the MSIX Packaging Tool | 1. Launch the **Internet Explorer** and browse to <https://www.microsoft.com/en-us/p/msix-packaging-tool/9n5lw3jbcxkf?activetab=pivot:overviewtab> 2. Enter a **MSA account** and click **Sign up**. 3. Click **Close**. 4. Click **Get**. 5. Click **Get** again on the Microsoft Store page. 6. Click **Sign in** and once again enter your **MSA account**. Click **Next**. 7. Enter your **MSA password** and click **Sign in**. 8. Click **Next** again. 9. The MSIX Packaging Tool will download and install. Close all the windows. |
| Download the XML Notepad 2007 MSI Installer and Create a Folder for the MSIX Package | 1. Launch the **Internet Explorer** and browse to <https://www.microsoft.com/en-in/download/details.aspx?id=7973> to download the XML Notepad 2007 MSI installer. 2. Click **Download** and save the installer in **C:\Packages** after creating the **Packages** folder in case the folder is not created. 3. Open **File Explorer** and navigate to **C:\Packages**. 4. Create a folder by the name **XMLNotepadMSIX**. |
| Create a PFX Certificate for the Application | 1. Click **Start** and search for **PowerShell**. Right-click **Windows PowerShell** and click **Run as administrator**. Accept the UAC prompt if required. 2. Execute the first command to create a new self-signed certificate: **New-SelfSignedCertificate -Type Custom -Subject "CN=Microsoft, O=Microsoft Corporation, C=US" -KeyUsage DigitalSignature -FriendlyName "XMLNotepad" -CertStoreLocation "Cert:\LocalMachine\My"** 3. Then execute the second command to set a password into a variable: **$pwd = ConvertTo-SecureString -String P@ssw0rd -Force -AsPlainText** 4. Then finally execute the third command to export the PFX certificate: **Export-PfxCertificate -cert "Cert:\LocalMachine\My\<Certificate Thumbprint as displayed in the output of the first command>" -FilePath C:\Packages\XMLNotepadMSIX\XMLNotepad.pfx -Password $pwd** 5. At this stage, you have a PFX certificate for the application that will be required by the MSIX Packaging Tool. |
| Trust the Certificate | 1. Right-click on **Start** and click **Run**. 2. Enter **mmc** and click **OK**. Accept the UAC prompt if required. 3. Click **File | Add/Remove Snap-in...** 4. Select **Certificates** and click **Add**. 5. Select **Computer account** and click **Next**. 6. Select **Local computer: (the computer this console is running on)** and click **Finish**. 7. Click **OK**. 8. Expand **Certificates (Local Computer) | Personal | Certificates**. 9. Right-click the **PFX** certificate that was created and click **All Tasks | Export...** 10. Click **Next**. 11. Select **No, do not export the private key** and click **Next**. 12. Select **DER encoded binary X.509 (.CER)** and click **Next**. 13. Click **Browse...** and navigate to **C:\Packages\XMLNotepadMSIX**, enter the **File name: XMLNotepad** and click **Save**. 14. Click **Next**. 15. Click **Finish**. 16. Click **OK** and close **MMC** without saving. 17. Open **File Explorer** and navigate to **C:\Packages\XMLNotepadMSIX** and double-click on the **.CER** file **XMLNotepad**. Not the .PFX file. 18. Click **Install Certificate...** 19. Select **Local Machine** and click **Next**. Accept the UAC prompt if required. 20. Select **Place all certificates in the following store** and click **Browse...** 21. Select **Trusted Root Certification Authorities** and click **OK**. 22. Click **Next**. 23. Click **Finish**. 24. Click **OK** and then click **OK** again. |
| Package and Convert the Win32 Application using the MSIX Packaging Tool | 1. Patch the VM completely and reboot until fully updated. 2. Click **Start** and then click **MSIX Packaging Tool** to launch the tool. Accept the UAC prompt if required. Select **Decline** for sending diagnostic data. 3. Click **Application package**. 4. On the Select environment screen, select **Create package on this computer** and then click **Next**. 5. On the Prepare computer screen, wait until the **MSIX Packaging Tool Driver** is **Installed**. It may also show that it is already installed. 6. If the **Windows Search is active** is displayed, select it and click **Disable selected**. 7. On the Prepare computer screen, click **Next**. 8. On the Select installer screen, click **Browse...** 9. Navigate to **C:\Packages** and select **XmlNotepad.msi**. Click **Open**. 10. Under Signing preference, select **Sign in with a certificate (.pfx)** and click **Browse...** 11. Navigate to **C:\Packages\XMLNotepadMSIX** and select the **.PFX** file. Click **Open**. 12. Enter the **password** that you set earlier in the second command. 13. On the Select installer screen, click **Next**. 14. On the Package information screen, rectify the values auto-populated. Ensure you have the following values: 15. Package name: **XML-Notepad-2007** 16. Package display name: **XML Notepad 2007** 17. Publisher name: **CN=Microsoft, O=Microsoft Corporation, C=US** 18. Publisher display name: **Microsoft Corporation** 19. Version: **2.3.0.0** 20. For the Installation location, click **Browse...** 21. Navigate to **C:\Program Files (x86)** and click **OK**. 22. On the Package information screen, click **Next**. 23. The XML Notepad 2007 Setup wizard will start. Click **Next** on the wizard. 24. Select **I accept the terms in the License Agreement** and click **Next**. 25. Click **Next** and then click **Install**. 26. Click **Finish** once XML Notepad 2007 is installed. Close the Internet Explorer window when it pops up. 27. On the Installation screen, click **Next**. 28. On the First launch tasks screen, click **Next**. 29. On the Are you done? screen, click **Yes, move on**. 30. On the Services report screen, click **Next**. 31. On the Create package screen, under Save location, click **Browse...** 32. Navigate to **C:\Packages\XMLNotepadMSIX** and click **Save**. 33. Click **Create**. 34. Once the package is created, on the MSIX Packaging Tool screen, click **Close** and close the MSIX Packaging Tool. |
| Uninstall the XML Notepad 2007 Win32 App | 1. Right-click on **Start** and click **Run**. 2. Enter **appwiz.cpl** and click **OK**. 3. Select **XML Notepad 2007** and click **Uninstall**. Click **Yes** and accept the UAC prompt if required. |
| Install the XML Notepad 2007 MSIX App | 1. Open **File Explorer** and navigate to **C:\Packages\XMLNotepadMSIX** and double-click on the **MSIX Installer** to install the application. Notice the new installation window for MSIX. 2. Click **Install**. You will see a progress bar showing the installation status.   **Note:** You might have to download and install the prerequisites for the app to launch, which it will do automatically, which is .Net Framework 3.5 (includes 2.0 and 3.0).   1. Once the prerequisite for the app is installed you can then re-launch the app from the **Start** menu. 2. Also note that in the **Programs and Features**, the application does not exist and can be uninstalled from the **Start** menu itself. |

# Deploy Windows 10

Organizations have traditionally been deploying new versions of Windows through the wipe and load approach using a standard image, Windows Assessment and Deployment Kit, Windows Deployment Services, Microsoft Deployment Toolkit and Configuration Manager.

We’ll also cover modern device deployment. With Windows 10, you can continue to use on-premises OS deployment, but you can also “manage out of the box.” AutoPilot transforms new devices into fully-configured, fully-managed devices. For existing devices running Windows 7 or Windows 8.1, you can use the robust in-place upgrade process for a fast, reliable move to Windows 10 while automatically preserving all the existing apps, data, and settings.

**Note:** If **CM1** is going to be used for deployments, then **MDT1** should be stopped. If **MDT1** is going to be used for deployments, then **CM1** should be stopped.

## OS Deployment Task Sequences in Configuration Manager

### Bare Metal

This section describes how to configure Configuration Manager for Bare Metal Operating System Deployment. This is the scenario used to deploy an image to a clean disk, or to reimage a computer where you don’t intend to keep any of the data on the disk.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

#### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Prerequisite Lab** | Complete **Section 9.1** OS Image Creation. |
| **Revert Virtual Machines** | On **CLIENT5**, revert to the first checkpoint. |
| **Complete these steps on the MDT1 virtual machine.** | |
| Disable Windows Deployment Services | 1. Right-click on the **Start** button and click **Run**. 2. Enter **services.msc** and then click **OK**. 3. On the Services MMC, look for **Windows Deployment Services Server**, right-click on it and select **Properties**. 4. Under Startup type, select **Disabled**. 5. Click **Stop**. 6. Click **Apply** and then **OK**. |
| **Complete these steps on the DC1 virtual machine.** | |
| Create Devices OU (if not already created) | 1. Logon to **DC1** as a domain administrator (**CORP\LabAdmin**). 2. On the Start screen, open the **Active Directory Users and Computers** MMC. 3. Right-click on **corp.contoso.com** and select **New >** **Organizational Unit**. You might have to expand **corp.contoso.com**. 4. Under Name, enter **Devices** and then click **OK**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create Folders | 1. Open **File Explorer** and browse to **C:\Packages**. 2. Create the folders with the following names:  * **MDTBootx64** * **MDTFiles** * **WIN10X64** * **WIN10X64-Settings** |

#### Create Task Sequence

In this activity, you will configure an MDT-based task sequence in Configuration Manager to deploy the reference image created earlier.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure Configuration Manager Integration | 1. On the Start screen, click **Configure ConfigMgr Integration** and click **Yes** on the UAC prompt. 2. Ensure that **Install the MDT extensions for Configuration** **Manager** is selected and within that **Install the MDT console extensions for System Center Configuration Manager** is selected and **Add the MDT task sequence actions to a System Center Configuration Manager server** is selected as well. 3. Ensure that the Site server name: shows **CM1.corp.contoso.com**. 4. Enter the Site code: **CHQ** if required and click **Next**. 5. Click **Finish**. |
| Create the Deployment Task Sequence, Boot Image and Related Packages | 1. On **CM1**, switch to the **Configuration Manager Console** by launching it with elevated rights. Click **Yes** on the UAC prompt if required. 2. In the console, click **Software Library**. 3. Click **Operating Systems >** **Task Sequences**. 4. On the ribbon click **Create MDT Task Sequence**. 5. In the Create MDT Task Sequence dialog, on the Choose Template page, select **Client Task Sequence** and click **Next**. 6. On the General page, type a Task sequence name of **Deploy Windows 10 X64** and click **Next**. 7. On the Details page, click to select the **Join a domain** radio button and configure the following values:   Domain: **Corp.contoso.com**.   1. Next to Account, click **Set**…   User name: **Corp\LabAdmin**.  Password/Confirm password: ***<provided by the customer>***.   1. Click **OK**.   User name: **Windows User**  Organization name: ***Customer name***.   1. Click **Next**. 2. On the Capture Settings page, ensure that **This task sequence will never be used to capture an image** is selected and click **Next**. 3. On the Boot Image page, click to select the **Create a new boot image package** radio button. 4. In Package source folder to be created field, type **\\CM1\Packages$\MDTBootx64** and click **Next**. 5. On the General Settings page, enter a Name of **MDT Boot Image (x64)** and click **Next**. 6. On the Options page, select **x64** and click **Next**. 7. On the Components page, leave the default feature packs and click **Next**. 8. On the Customization page, leave the default customizations and click **Next**. 9. On the MDT Package page, click to select the **Create a new Microsoft Deployment Toolkit Files package** radio button. 10. In Package source folder to be created field, type **\\CM1\Packages$\MDTFiles** and click **Next**. 11. On the MDT Details page, enter a Name of **MDT Files** and click **Next**. 12. On the OS Image page, select **Create a new OS image** and configure the following values and click **Next**:   OS image file (WIM) location: **\\MDT1\Create$\Captures\WIN10REF\ICS002.wim**.  Package source folder to be created: **\\CM1\Packages$\WIN10X64**.   1. On the Image Details page, enter a Name of **Windows 10 - x64** and click **Next**. 2. On the Deployment Method page, ensure that **Perform a “Zero Touch Installation” OS deployment, with no user interaction** is selected and then click **Next**. 3. On the Client Package page, click **Browse**… for the option **Specify an existing ConfigMgr client package**. 4. In the Select a Package dialog, select **Microsoft Corporation Configuration Manager Client Package** and click **OK**. 5. Click **Next**. 6. On the USMT Package page, click **Browse**… for the option **Specify an existing USMT package**. 7. In the Select a Package dialog, select **Microsoft Corporation User State Migration Tool for Windows 10.0.19041.1** and click **OK**. Click **Next**. 8. On the Settings Package page, click to select the **Create a new settings package** radio button. 9. In the Package source folder to be created field, type **\\CM1\Packages$\WIN10X64-Settings** and click **Next**. 10. On the Settings Details page, enter a Name of **Windows 10 X64 Settings** and click **Next**. 11. On the Sysprep Package page, ensure that **No Sysprep package is required** radio button is selected and click **Next**. 12. Review the Summary details and click **Next**.   **Note**: It can take up to five minutes for the boot image to be created.   1. On the Confirmation page, confirm that the wizard completed successfully and click **Finish**. |
| Distribute the Task Sequence Package to the Distribution Point | 1. In the results pane, select **Deploy Windows 10 X64** task sequence. 2. On the ribbon, click **Distribute Content**. 3. On the General page, click **Next**. 4. On the Content page, click **Next**. 5. On the Content Destination page, click **Add >** **Distribution Point**. 6. On the Add Distribution Points dialog, click to select the **\\CM1.CORP.CONTOSO.COM** checkbox and click **OK**. 7. Click **Next**. 8. Review the Summary details and click **Next**. 9. On the Completion page, confirm that the wizard completed successfully and click **Close**. Ensure that all the content has been distributed to the distribution point from the **Monitoring > Distribution Status >** **Content Status**. |
| Deploy the Task Sequence to the Unknown Computers Collection | 1. In the results page, select the **Deploy Windows 10 X64** task sequence. 2. On the ribbon click **Deploy**. 3. On the General page, next to Collection, click **Browse**… Click **OK** on the notification that appears. 4. In the Select Collection dialog, click the **All Unknown Computers** collection and click **OK**. 5. Click **Next**. 6. On the Deployment Settings page, in the Make available to the following: drop down list select **Configuration Manager clients, media and PXE**. 7. Click **Next**. 8. On the Scheduling page, click **Next**. 9. On the User Experience page, click **Next**. 10. On the Alerts page, click **Next**. 11. On the Distribution Points page, click **Next**. 12. Review the Summary details and click **Next**. 13. On the Completion page, confirm that the wizard completed successfully and click **Close**. |
| Add the Boot Image to the Distribution Point | 1. In the **Software Library** pane, expand **Operating Systems** and click **Boot Images**. 2. In the results pane, click **MDT Boot Image (x64)**. 3. On the ribbon click **Properties**. 4. In the properties dialog, click the **Data Source** tab. 5. Click to select the **Deploy this boot image from the PXE-enabled distribution point** check box. 6. For **Architecture**, select **x64** and for **Language**, select **English (United States)**. 7. Click **Apply** and then **OK**. |
| Edit the Task Sequence – Administrator Password | 1. In the **Software Library** pane, expand **Operating Systems** and click **Task Sequences**. 2. Select **Deploy Windows 10 X64** and click **Edit** from the ribbon bar. 3. Navigate to **Post Install >** **Apply Windows Settings**. 4. Select the option, **Enable the account and specify the local administrator password**, enter the password ***<provided by the customer>*** in the Password and Confirm password fields. |
| Edit the Task Sequence – Machine Object OU | 1. Navigate to **Post Install >** **Apply Network Settings**. 2. Click **Browse**… for the Domain OU field and select the **Devices** OU for deployments and click **OK**. Click **Apply** and **OK**. |
| Configure the Distribution Point with PXE and Multicast Option | 1. Navigate to **Administration >** **Distribution Points**. 2. Right-click **CM1.CORP.CONTOSO.COM** and click **Properties**. 3. Click the **PXE** tab, check the box next to **Enable PXE support for clients**, click **Yes** on the prompt, and check the boxes next to **Allow this distribution point to respond to incoming PXE requests**, **Enable unknown computer support**, click **OK** on the prompt again and check the box next to **Enable a PXE responder without Windows Deployment Service** and finally click **Yes** on the prompt again. Uncheck the box next to **Require a password when computers use PXE**. 4. Click **Apply** and then click **OK**. |

#### Deploy Windows on an Unknown Computer

This activity will initiate and complete the process to deploy the reference Windows system image through Bare Metal Deployment. At the end of the activity, CLIENT5 will be installed with the reference system image.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT5 virtual machine.** | |
| PXE Boot and Commence OSD | 1. Power on the **CLIENT5** virtual machine and when prompted, press **F12** for network service boot to boot from the boot image available from the PXE distribution point. 2. On the Welcome to the Task Sequence Wizard page, click **Next**. 3. On the Select a task sequence to run page, ensure that **Deploy Windows 10 X64** is selected and click **Next**. 4. The system will now complete the installation of Windows on the virtual machine but the application XML Notepad 2007 will not be deployed as part of the image as it is not captured initially. Also, once the deployment is finished, ensure that the deployment status in Configuration Manager shows **Successful** from **Monitoring >** **Deployments** as well as the machine has a correct status in Configuration Manager from **Assets and Compliance >** **Devices**. Additionally, reboot the client machine once, after the deployment so that the **Configuration Manager Client** shows all the **tabs** and the **Action Tasks** is **fully initialized,** and the **Software Center** is there as well.   **Note**: The system will be named with a MININT-<random number>. |

### PC Refresh

In this section, we will refresh a Windows 7 client with Windows 10, keeping all data intact.

**Prerequisites:**

1. Complete **OS Image Creation**.
2. Complete **Bare Metal**.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the WIN7 and CLIENT1 virtual machines.** | |
| Copy User Data for Migration during a Refresh | 1. Log in to **CLIENT1** and **WIN7** as **CORP\LabAdmin**. 2. Copy the contents of the **CLIENT1** - **Desktop**, **Documents** and **Pictures** from **C:\Users\LabAdmin** to the same locations in **WIN7**. 3. Create another virtual machine checkpoint on **WIN7**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Refresh Device Collection | 1. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **Refresh**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule | Direct Rule** and click **Next** on the Welcome page. 2. In the Search for Resources page, in the Value, enter **WIN7** and then click **Next**. 3. In the Select Resources page, select **WIN7** and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. 6. Back on the Membership Rules page, click **Next**. 7. On the Summary page, click **Next**. 8. On the Completion page, click **Close**. 9. Ensure that the **WIN7** machine is present in the **Refresh** collection. |
| Create a Refresh Task Sequence Deployment | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Deploy Windows 10 X64** Task Sequence and click **Deploy**. 3. On the General page, click **Browse...** 4. Click **OK** on the prompt. 5. Select **Refresh** and then click **OK**. 6. Back on the General page, click **Next**. 7. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Only Configuration Manager Clients** is selected next to Make available to the following. Click **Next**. 8. On the Scheduling page, click **Next**. 9. On the User Experience page, click **Next**. 10. On the Alerts page, click **Next**. 11. On the Distribution Points page, click **Next**. 12. On the Summary page, click **Next**. 13. On the Completion page, click **Close**. |
| **Complete these steps on the WIN7 virtual machine.** | |
| Execute the Refresh Task Sequence Deployment | 1. Click **Start | Control Panel**. 2. Click **System and Security | Configuration Manager**. 3. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 4. Click **Run Now** and then click **OK**. 5. Click the **notification** or open the **Software Center**. 6. Under Operating Systems select **Deploy Windows 10 X64** and then click **Install**. 7. Click **Install** again on the prompt. 8. Notice that the **WIN7** machine installed with Windows 7 will be refreshed with Windows 10 and all user data will be backed up and restored using the User State Migration Tool as part of **PC Refresh**. |

### PC Replacement

In this section, we will replace a Windows 7 client with a new Windows 10 client, keeping all data intact.

**Prerequisites:**

1. Complete **Section 9.1 - OS Image Creation**.
2. Complete **Section 9.2.1 - Bare Metal**.
3. Complete **Section 7.2.1 or 9.2.2 – PC Refresh**.

**Note:** On **WIN7**, revert to the latest checkpoint.

**Some Workarounds:**

1. When you try to deploy the **Replace Task Sequence** on the Source Computer (**WIN7**) once again or the second time, it might fail accessing the State Migration Point share. The workaround is:
2. Remove the **State Migration Point Role** and delete any folder(s) inside **C:\MigData**.
3. On **WIN7**, in the registry, delete any key(s) under **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SystemCertificates\SMS\Certificates** and reboot **WIN7**.
4. When you deploy the **Windows 10 X64 Task Sequence** on the Destination Computer (**CLIENT6**), it might fail to restore the local computer user profile. The workaround is:
5. Edit the **Windows 10 X64 Task Sequence** and under the **State Restore** Group, select **Restore User State** step.
6. Select **Restore local computer user profiles** and enter the **password** of the **local user account** of the Source Computer (**WIN7**) twice.

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the CM1 virtual machine.** | | |
| Install the State Migration Point | 1. In the Configuration Manager Console, browse to **Administration | Site Configuration | Servers and Site System Roles**. 2. Right-click **CM1.corp.contoso.com** and then click **Add Site System Roles**. 3. On the General page, click **Next**. 4. On the Proxy page, click **Next**. 5. On the System Role Selection page, select **State migration point** and click **Next**. 6. Manually create a folder in **C:\** drive called **MigData** and then on the State migration point page, click the **star** symbol. 7. For the Storage folder, enter **C:\MigData** and click **OK**. 8. On the State migration point page, click **Next**. 9. On the Boundary Groups page, click **Next**. 10. On the Summary page, click **Next**. 11. On the Completion page, click **Close**. | |
| Create a Replace Task Sequence | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Click **Create MDT Task Sequence** from the ribbon bar. 3. On the Choose Template page, select **Client Replace Task Sequence** and click **Next**. 4. On the General page, for the Task sequence name, enter **Replace Task Sequence** and then click **Next**. 5. On the Boot Image page, select **Specify an existing boot image package** and then click **Browse...** 6. Select **MDT Boot Image (x64) en-US** and then click **OK**. 7. Click **Next** on the Boot Image page. 8. On the MDT Package page, select **Specify an existing Microsoft Deployment Toolkit Files package** and then click **Browse...** 9. Select **MDT Files** and then click **OK**. 10. Click **Next** on the MDT Package page. 11. On the USMT Package page, select **Specify an existing USMT package** and then click **Browse...** 12. Select **Microsoft Corporation User State Migration Tool for Windows 10.0.19041.1** and then click **OK**. 13. Click **Next** on the USMT Package page. 14. On the Settings Package page, select **Specify an existing settings package** and then click **Browse...** 15. Select **Windows 10 X64 Settings** and then click **OK**. 16. Click **Next** on the Settings Package page. 17. On the Summary page, click **Next**. 18. On the Confirmation page, click **Finish**. | |
| Create a Replace Device Collection | 1. Browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **Replace**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule | Direct Rule** and click **Next** on the Welcome page. 2. In the Search for Resources page, in the Value, enter **WIN7** and then click **Next**. 3. In the Select Resources page, select **WIN7** and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. 6. Back on the Membership Rules page, click **Next**. 7. On the Summary page, click **Next**. 8. On the Completion page, click **Close**. 9. Ensure that the **WIN7** machine is present in the **Replace** collection. | |
| Create a New Computer Device Collection | 1. Browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **New Computer**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Next**. Click **OK** on the prompt. 2. On the Summary page, click **Next**. 3. On the Completion page, click **Close**. | |
| Associate CLIENT6 with WIN7 | 1. On the Hyper-V Host, start **CLIENT6** for a moment to get the MAC Address of the VM from the **Networking** tab at the bottom and make a note of it. Once noted, turn off **CLIENT6**. 2. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | Devices**. 3. Right-click **Devices** and then click **Import Computer Information**. 4. On the Select Source page, select **Import single computer** and then click **Next**. 5. On the Single Computer page, enter the following and then click **Next**:   Computer name: **CLIENT6**  MAC address: Enter the **MAC Address** which you noted in **Step 48**  Source computer: Click **Search...**, next to Collection click **Browse...**, select **All Systems**, click **OK**, enter **WIN7** next to Computer contains, click **Search**, select **WIN7** from the search results and then click **OK**.   1. On the User Accounts page, under Migration behavior, select **Capture and restore all user accounts** and then click **Next**. 2. On the Data Preview page, click **Next**. 3. On the Collections page, click **Add**, select **New Computer**, click **OK**, select **New Computer** again and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Confirmation page, click **Close**. 6. Click **User State Migration** and review the computer association in the right pane. 7. Select **WIN7/CLIENT6** association and click **View Recovery Information** from the ribbon bar. Note that a user state recovery key has been assigned already, but a user state store location has not. Click **Close**. 8. Ensure that the All Systems collection has the **CLIENT6** VM in it. | |
| Create a Replace Task Sequence Deployment | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Replace Task Sequence** and click **Deploy**. 3. On the General page, click **Browse...** 4. Click **OK** on the prompt. 5. Select **Replace** and then click **OK**. 6. Back on the General page, click **Next**. 7. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Only Configuration Manager Clients** is selected next to Make available to the following. Click **Next**. 8. On the Scheduling page, click **Next**. 9. On the User Experience page, click **Next**. 10. On the Alerts page, click **Next**. 11. On the Distribution Points page, click **Next**. 12. On the Summary page, click **Next**. 13. On the Completion page, click **Close**. | |
| **Complete these steps on the WIN7 virtual machine.** | | |
| Execute the Replace Task Sequence Deployment | | 1. Click **Start | Control Panel**. 2. Click **System and Security | Configuration Manager**. 3. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 4. Click **Run Now** and then click **OK**. 5. Click the **notification** or open the **Software Center**. 6. Under Operating Systems select **Replace Task Sequence** and then click **Install**. 7. Click **Install** again on the prompt and wait for the task sequence to complete after reboot and re-log in. |
| **Complete these steps on the CM1 virtual machine.** | | |
| Verify the Backup | | 1. Browse to **C:\MigData** and verify that a folder was created containing the USMT backup. 2. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | User State Migration**. 3. Select **WIN7/CLIENT6** association and click **View Recovery Information** from the ribbon bar. Note now that a user state store location has been set as well. Click **Close**. |
| Deploy the New Computer CLIENT6 | | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Deploy Windows 10 X64** Task Sequence and click **Edit**. 3. Under the **State Restore** Group, select **Restore User State** step. 4. Select **Restore local computer user profiles** and enter the **password** of the **local user account** of the Source Computer (**WIN7**) twice. Click **Apply** and **OK**. 5. Right-click **Deploy Windows 10 X64** Task Sequence and click **Deploy**. 6. On the General page, click **Browse...** 7. Click **OK** on the prompt. 8. Select **New Computer** and then click **OK**. 9. Back on the General page, click **Next**. 10. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Configuration Manager clients, media and PXE** is selected next to Make available to the following. Click **Next**. 11. On the Scheduling page, click **Next**. 12. On the User Experience page, click **Next**. 13. On the Alerts page, click **Next**. 14. On the Distribution Points page, click **Next**. 15. On the Summary page, click **Next**. 16. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT6 virtual machine.** | | |
| Execute the New Computer Task Sequence Deployment | | 1. Power on the **CLIENT6** virtual machine and when prompted, press **F12** for network service boot to boot from the boot image available from the PXE distribution point. 2. On the Welcome to the Task Sequence Wizard page, click **Next**. 3. On the Select a task sequence to run page, ensure that **Deploy Windows 10 X64** is selected and click **Next**. 4. When the process is complete, you will have a new Windows 10 machine in your domain with user data and settings restored from **WIN7**. |

### Upgrade

For existing computers running Windows 7, Windows 8, or Windows 8.1, the recommended path for deploying Windows 10 leverages the Windows installation program (Setup.exe) to perform an in-place upgrade, which automatically preserves all data, settings, applications, and drivers from the existing operating system version. This requires the least effort, because there is no need for any complex deployment infrastructure.

In this section, you will go through the process of automating the upgrade process through Configuration Manager for enterprise wide deployments or, optionally, performing manual upgrade for very small scale scenarios. At the end of the section, the device will be upgraded to Windows 10.

**Note**: The Trial Download of the Windows 10 Enterprise Media does not allow an In-Place Upgrade to be performed. To complete this lab, Windows 10 Enterprise Media must be sourced from either MSDN Subscriber Downloads or from the Volume Licensing Site of the customer.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

**Note:** On **WIN7**, revert to the first checkpoint. Ensure it is in a cleaned state with no incompatible software installed. Software that can conflict can be antivirus or firewall software which should be uninstalled if they exist. Also, during applying the checkpoints back and forth, there is a possibility that the VM loses domain trust relationship. In that case, disjoin and then rejoin the VM to the domain. While doing so, ensure that VM is cleaned up in AD and ConfigMgr and after the domain-join the VM shows active in both AD and ConfigMgr.

#### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Download the Latest MSDN Version of Windows 10 Enterprise | 1. Open **File Explorer** then browse to **C:\Packages**. 2. On the **Packages** folder, create a folder named **Windows 10 MSDN**. 3. Open Internet Explorer and browse to the URL below.   <https://msdn.microsoft.com/subscriptions/securedownloads/>   1. From the website, Sign-in with your MSDN registered account. 2. On the **Search** field, enter **Windows 10**. 3. **Search** for **Windows 10 (business editions), version 21H1 (*Latest Available Update*) (x64) – DVD (English)** and **Download** to **C:\Packages\Windows 10 MSDN**. |

#### Perform an In-Place Upgrade of Windows 7 Using Configuration Manager (Current Branch)

This activity will perform an in-place upgrade of the Windows 7 device to Windows 10 using Configuration Manager (current branch).

**Note**: Only perform this activity if the Configuration Manager is on the latest Current Branch.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Import the Windows 10 Upgrade Package | 1. Navigate to **C:\Packages\Windows 10 MSDN** and mount the **ISO**. 2. Navigate to **C:\Packages** folder and create a folder named **Windows10Media**. 3. Copy the contents of the mounted ISO to **C:\Package\Windows10Media**. 4. **Eject** the ISO and **delete** the **C:\Packages\Windows 10 MSDN** folder. 5. Open the **Configuration Manager Console**, browse to **Software Library > Operating Systems >** **Operating System Upgrade Packages**. 6. Click **Add Operating System Upgrade Package** from the ribbon bar. 7. On the **Data Source** page, under **Path** enter **\\CM1\Packages$\Windows10Media**, select **Extract a specific image index from install.wim file of selected upgrade package**, select **3 – Windows 10 Enterprise** next to **Image index**, select **x64** next to **Architecture** and select **English (United States)** next to **Language** and then click **Next**. 8. On the **General** page, under **Name** enter **Windows 10 21H1 x64** then click **Next**. 9. On the **Summary** page, click **Next**. 10. Once complete, click **Close**. |
| Create an Upgrade Task Sequence | 1. On the **Configuration Manager Console**, switch to the **Software Library** workspace, expand **Operating Systems**, right-click **Task Sequences**, and select **Create Task Sequence**. 2. On the **Create a new task sequence** page, select **Upgrade an operating system from an upgrade package** then click **Next**. 3. On the **Specify task sequence information**, under **Task sequence name** enter **Upgrade to Windows 10** then click **Next**. 4. On the **Select an operating system upgrade package** page, click **Browse**. 5. On the **Select an Operating System Upgrade Package** window, select **Windows 10 21H1 x64 en-US** then click **OK**. 6. For **Specify the edition index and licensing information for this upgrade package, if required**, ensure that **3 – Windows 10 Enterprise** is selected from the dropdown. 7. On the **Select an operating system upgrade package** page, click **Next**. 8. On the **Include software updates** page, click **Next**. 9. On the **Install applications** page, click **Next**. 10. On the **Summary** page, click **Next**. 11. Once complete, click **Close**. |
| Distribute Content to DPs | 1. On the **Configuration Manager Console**, switch to the **Software Library** workspace, expand **Operating Systems >** **Task Sequences**, right-click **Upgrade to Windows 10** and select **Distribute Content**. 2. Enter the following information:   *General* – Click **Next**.  *Content* –Click **Next**.  *Content Destination* – Click **Add >** **Distribution Point**.  Select **CM1.CORP.CONTOSO.COM** and click **OK** and then click **Next**.  *Summary* – Click **Next**, click **Close**. Ensure that the content is distributed from the **Monitoring > Distribution Status >** **Content Status**. |
| Create a Collection to Deploy the Task Sequence | 1. Select the **Assets and Compliance** workspace and select **Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. Input the following information:   *General*  Name – Enter **In-Place Upgrade**.  Limiting collection – Select **All Desktop and Server Clients** and click **Next**.  Select **Use incremental updates for this collection**.  Click **Next**.  Accept the Warning.  *Summary* – click **Next**, click **Close**. |
| Add the Windows 7 Device to the Collection | 1. In the **Assets & Compliance** workspace, select **Devices** and right-click **WIN7**. 2. Select **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 3. Select **In-Place Upgrade** and click **OK**. 4. Select **Device Collections**, right-click **In-Place Upgrade**, and select **Update Membership**. Click **Yes** on the warning box to continue. |
| Deploy the Task Sequence | 1. Select **Software Library > Operating Systems >** **Task Sequences**. 2. Right-click the **Upgrade to Windows 10** task sequence and select **Deploy**. 3. Enter the following information:   General – Collection – select **Browse**… click **OK** on the warning and select **In-Place Upgrade** collection. Click **OK** and then click **Next**.   1. On the Deployment Settings page, specify the following information:   Purpose: Choose **Required**.  Then click **Next**.   1. On the Scheduling page, specify the following information:   Click **New (**next to Assignment schedule) and select **Assign immediately after this event**. Accept the defaults, click **OK**.  Rerun behavior: Set to **Rerun if failed previous attempt**.  Then click **Next**.   1. On the User Experience Page, keep the default settings and click **Next**. 2. On the Alerts Page, keep the default settings and click **Next**. 3. On the Distribution Points page, specify the following information:   Deployment options: Choose **Download content locally when needed by the running task sequence**.   1. Click **Next**, click **Next** again and then click **Close** to finish the deployment Wizard. |
| **Complete these steps on the WIN7 virtual machine.** | |
| Refresh Policy on the Windows 7 Device | 1. On the Windows 7 device, logon as **corp\labadmin** and open the **Control Panel**. Select the **Configuration Manager** icon. 2. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run** **Now** to force the device to receive updated policy. This can take up to 5 minutes.   **Note**: As soon as the deployment is available, it will then retry to start the installation after few minutes. The In-Place Upgrade Task sequence will now initiate and upgrade the Windows 7 device to Windows 10 without further user intervention. If required, restart the SMS Agent Host Service to trigger the process.  **Note:** In case you get the error **0x80004005** during the upgrade process, look for the following programs in **Add/Remove Programs – System Center Endpoint Protection and Windows Firewall Configuration Provider**. If they are present, uninstall both, reboot the VM once and try re-deploying the task sequence. |

#### Manual Upgrade

In this section, you will perform a manual in-place upgrade to Windows 10 on a Customer-Provided device. The requirements are as follows:

* Customer Provided Devices (Reference Devices) with a Corporate Image pre-installed.
* The pre-installed Corporate Image must be Windows 7 or later.
* Windows 10 Installation Files.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Device provided by the Customer.** | |
| Extract Windows 10 Media | 1. Extract the files from Windows 10 ISO to a USB drive. The ISO is the downloaded **Windows 10 (business editions), version 21H1 (*Latest Available Update*) (x64) – DVD (English)** from MSDN. |
| Perform Manual In-Place Upgrade | 1. Insert the USB drive into the reference device that will be upgraded. 2. Navigate to the drive using Windows Explorer. 3. Start **setup.exe** with elevated rights from the USB drive and accept the UAC prompt. 4. Review any options and compatibility information that is provided. 5. Complete the upgrade. 6. Evaluate the system to ensure that migrated applications and data are retained. 7. Investigate applications that were installed in the corporate image and note any incompatibilities. |

## OS Deployment Task Sequences in MDT

This section describes how to configure Microsoft Deployment Toolkit for Operating System Deployment.

**Note:** On **CLIENT6**, revert to the first checkpoint. Also, in **MDT1**, if you have disabled and stopped the **Windows Deployment Services Server** from previous labs, then change it to **Automatic** and **Start** the service.

### Prepare a Windows 10 Operating System Deployment

This activity will import the reference Windows system image and configure an operating system deployment task sequence.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the MDT1 virtual machine.** | |
| Add the Reference Image to the Deployment Share | **Note**: Steps 1 – 10 are only required if a new image was created from Section 9.1.   1. Open the MDT **Deployment Workbench** from the Start Menu and click **Yes** on the UAC prompt. 2. Expand **Image Deployment (\\MDT1\Deploy$)**. 3. Expand **Operating Systems**. 4. Expand **Custom Image Files** and then select **Windows 10**. 5. In the Actions Pane on the right, click **Import Operating System**. 6. In the OS Type pane, select **Custom image file**. Click **Next**. 7. In the Image pane, click **Browse**… Navigate to **C:\DS-Create\Captures\WIN10REF**. 8. Select the **ICS002.wim** created in the previous activity. Click **Open**. Click **Next**. 9. Complete the Wizard with the default options. 10. The custom image is now imported into the Workbench. |
| Update the Task Sequence to use the New Image | 1. In the Deployment Workbench, select **Task Sequences**. 2. Select **Corporate x64 Windows 10 Enterprise**. Right-click and select **Properties**. 3. Click the **Task Sequence** tab. 4. Expand the **Install** task sequence group. 5. Select **Install Operating System**. 6. Click **Browse**… 7. Expand the nodes **Operating Systems > Custom Image Files >** **Windows 10** to locate and select the custom image imported in the previous task. Click **OK**. 8. Now, navigate to **State Restore >** **Custom Tasks** and select **Office 2013 C2R**, on the right, click the **Options** tab and check the box next to **Disable this step**. The reason is that the kit does not contain source files for Office 2013 applications and the deployment at the end will show errors regarding it. 9. Click **Apply**. Click **OK** to commit the change. 10. The task sequence is now ready for use to deploy to the reference system image. |

### Perform a Windows 10 Deployment

This activity will initiate and complete the process to deploy the reference Windows system image through the task sequence.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT6 virtual machine.** | |
| Boot from the Network (PXE) | 1. To avoid any conflicts between **MDT1** and **CM1** PXE boot, pause/stop the **CM1** VM. 2. Power on the **CLIENT6** virtual machine. 3. If prompted, press **F12** for network service boot. 4. At the Windows Boot Manager screen, select **Deploy - X64**. Press **Enter**. 5. The device will now perform a PXE boot in to Windows PE. |
| Initiate the Deployment of the Reference Image | 1. At the Task Sequence pane, select **Corporate x64 Windows 10 Enterprise** and click **Next**. 2. On the Computer Details page, change the User Name to **LabAdmin**, under Password enter ***<provided by the customer>*** and then click **Next**. 3. Keep the default setting for the Product Key and click **Next**. 4. Keep the default setting for Locale and Time and click **Next**. 5. For the Applications, ensure that none of the Office 2013 applications are selected and click **Next**. The reason is that the kit does not contain source files for Office 2013 applications and the deployment at the end will show errors regarding it. 6. When it asks for Administrator Password, enter ***<provided by the customer>*** two times and click **Next**. 7. In the BitLocker page, click **Next**. 8. At the Ready pane, click **Begin**. 9. The system will now commence the deployment of the reference Windows system image, but the application XML Notepad 2007 will not be deployed as part of the image as it is not captured initially. Once done, click **Finish**, and the virtual machine will automatically reboot. |

## Windows AutoPilot

Windows AutoPilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. In this section, you will use the Microsoft Intune to configure AutoPilot for pre-configuring devices.

**Note:** If **CLIENT4** is already existing in **Azure AD** and **Intune** from the previous labs, then remove it from both places and ensure that the device is un-enrolled.

### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the HYPER-V Host.** | |
| Create a Checkpoint in Hyper-V (if not already created) | 1. Open **Hyper-V Manager**. 2. Right-click on **HYD-CLIENT4** and select **Checkpoint**. |
| **Complete these steps on the CLIENT4 virtual machine.** | |
| Capture Device ID | 1. Login as the local administrator and open PowerShell as an administrator. Accept the UAC prompt if required. 2. Run the below commands and press **Y** and **A** wherever prompted. Install-Script –Name Get-WindowsAutoPilotInfo   Set-ExecutionPolicy Unrestricted   1. Change the directory to **C:\Program Files\WindowsPowerShell\Scripts** and run the below command.   **Note:** Ensure that **Windows Remote Management (WS-Management)** service is running on the machine for the script to be executed successfully. .\Get-WindowsAutoPilotInfo.ps1 -ComputerName CLIENT4 –OutputFile C:\Users\Administrator\Desktop\MyComputers.csv   1. Copy the MyComputers.csv file to the computer that will be used for Microsoft Intune setup. 2. Open Command Prompt as an administrator. Accept the UAC prompt if required. 3. Run the following command after changing the directory to **C:\Windows\System32\Sysprep** SYSPREP\Sysprep.exe /OOBE /SHUTDOWN |

### Set Intune as Management Authority

After you complete the following tasks, you are ready to manage mobile devices and computers.

| Task | | Detailed Steps | |
| --- | --- | --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | | |
| Enable Device Management. Set Mobile Device Management Authority (If MDM Authority is not equal to Intune) | **Note**: Before you can enroll mobile devices, you must prepare the Intune service by selecting the appropriate mobile device management authority setting on the Mobile Device Management page of the Administration workspace. The mobile device management authority setting determines whether you manage mobile devices with Intune or Configuration Manager with Intune integration. This guidance assumes Intune is used without Configuration Manager integration so the setting should be set to Microsoft Intune.   1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Select **Device enrollment**. 6. Under Mobile Device Management Authority, select **Intune MDM Authority** and click **Choose**. | |
| Create Groups (If not present) | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 5. Click **+ New group**. 6. In the Group pane fill in the following values:   Group type: **Microsoft 365**  Group name: **Sales**  Membership type: **Assigned**  Members: **Test User1** and **Test User2**   1. Click **Create**. | |
| Customize the Company Portal | 1. On the left navigation bar, click **All services > search and click Intune > Intune**. 2. Select **Client apps** > **Customization** and click **Edit**. 3. Under the **Settings** tab, customize the page as per your convenience. 4. Click **Review + save** and then click **Save**. 5. Click **Azure Active Directory > Company branding > Configure**. 6. Customize the page as per your convenience and then click **Save**. | |
| Verify the Company Portal Configuration | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.manage.microsoft.com> and Sign in with **TU1@<AzureDomainName>.onmicrosoft.com**. 4. Review the company portal, browse to **Helpdesk** from the top left-hand corner and confirm that the customizations have been applied. | |

### Enable Auto MDM Enrollment

In this activity, you will configure automatic MDM enrollment to Intune upon joining Azure AD.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure Auto MDM Enrollment for Intune (If not configured) | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune**. 5. In the **MDM user scope** setting, select **All**. 6. Click **Save**. |

### Add an App

In this activity, you will add an app to Intune which will automatically download once the device is enrolled into MDM.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Add an App (If not already done before) | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Select **Client apps** > **Apps**. 6. Click **+Add**. 7. In the App type dropdown, select **Line-of-business app** and click **Select**. |
| Configure App (If not already done before) | 1. Under **App information**, click **Select app package file**. 2. On the **App package file** blade, choose the browse button, and select a Windows installation file with the extension **.msi, .appx, or .appxbundle**. A sample msi file can be downloaded from: <https://www.7-zip.org/download.html> 3. Click **OK.** 4. Under **App information**, enter the following information and click **Next**:    1. **Name** - Enter the name of the app as it is displayed in the company portal. Make sure all app names that you use are unique. If the same app name exists twice, only one of the apps is displayed to users in the company portal.    2. **Description** - Enter a description for the app. The description is displayed to users in the company portal.    3. **Publisher** - Enter the name of the publisher of the app.    4. **App install context** – This specifies the install context to be associated with this app. For dual mode apps, select the desired context for this app. For all other apps, this is pre-selected based on the package and cannot be modified.    5. **Ignore app version** – Set this to “Yes” only for apps that are automatically updated by the app developer (such as Google Chrome).    6. **Command**-**line** **arguments** - Optionally, enter any command-line arguments that you want to apply to the .msi file when it runs, like /q.    7. **Category** - Select one or more of the built-in app categories, or a category you created. Categorizing apps makes it easier for users to find the app when they browse the company portal.    8. **Show this as a featured app in the Company Portal** - Display the app prominently on the main page of the company portal when users browse for apps.    9. **Information URL** - Optionally, enter the URL of a website that contains information about the app. The URL is displayed to users in the company portal.    10. **Privacy URL** - Optionally, enter the URL of a website that contains privacy information for the app. The URL is displayed to users in the company portal.    11. **Developer** - Optionally, enter the name of the app developer.    12. **Owner** - Optionally, enter a name for the owner of this app, for example, HR department.    13. **Notes** - Enter any notes you would like to associate with this app.    14. **Logo** - Upload an icon that is associated with the app. The icon is displayed with the app when users browse the company portal. |
| Deploy App (If not already done before) | 1. Under **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 2. Under **Review + create**, review the page and click **Create**.   **Note:** This group should have already been created as part of **Section 3.2.1**. |

### Configure AutoPilot

In this activity, you will configure automatic MDM enrollment to Intune upon joining Azure AD.

**Note:** If **CLIENT4** is already existing in **Azure AD** and **Intune** from the previous labs, then remove it from both places and ensure that the device is un-enrolled.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure AutoPilot | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to [https://www.portal.azure.com/](https://www.portal.azure.com/en-us/business-store) and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Click **Device enrollment** > **Windows enrollment** > **Devices**. 6. Click **Import,** and select the **MyComputers.csv** file saved from before and click **Import**. 7. Once imported, to speed up the process, click **Sync** and then click **Refresh** until you see the device. 8. Under the **Microsoft Intune** pane, click **Groups > + New group**. 9. Select **Group type – Security**, **Group name – AutoPilot Devices** and **Membership type – Assigned**. 10. Click **Members**, select the machine where the name equals the serial number of the device. Click **Select**. 11. Click **Create**. 12. On the **Device enrollment** > **Windows enrollment** pane, click **Deployment Profiles** > **+ Create profile**. 13. On the **Basics** tab, in the **Name** box, type **AutoPilot Test Profile** and click **Next**. 14. On the **Out-of-box experience (OOBE)** tab, in the **Deployment mode** dropdown, select **User-Driven**. 15. In the **Join to Azure AD as** dropdown, select **Azure AD joined**. 16. Select **Hide** for the **Microsoft Software License Terms** option. 17. Select **Hide** for the **Privacy Settings** option. 18. Select **Hide** for the **Hide change account options** option. 19. Select **Standard** for the **User account type** option and click **Next**. 20. In the **Assignments** tab, click **+ Select groups to include**, select the **AutoPilot Devices** group just created and click **Select** and then click **Next**. 21. In the **Review + create** tab, click **Create.** 22. Wait for some time for the device to be showing up in **Assigned devices** under **AutoPilot Test Profile**. To speed up the process, click **Sync** and then click **Refresh** in the **Device enrollment** > **Windows enrollment** > **Devices** pane, until you see the device there. 23. Click the **Devices** page, and you should be able to see the **PROFILE STATUS** as **Updating** and then further **Assigned**. Wait for a few moments. 24. Select the device imported and click **Assign user**. 25. Type in and select **Test User1** or **TU1@<AzureDomainName>.onmicrosoft.com** and click **Select**. Click **Save**. Wait for a moment while the device is assigned to the user. |

### AutoPilot for OOBE

In this activity, you will walk through the experience of self-service AutoPilot while in OOBE.

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from the CLIENT4 virtual machine.** | | |
| Perform Azure AD Join | | 1. Start the VM and once OOBE has started, in the **Hi Test User1! Welcome to Microsoft Services** pane, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**. 2. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 3. In the **All set!** pane, click **OK**. |
| Validate Azure AD Join and MDM Enrollment | | 1. Go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Confirm that **Connected to <CompanyName>’s Azure AD** is displayed and the **Info** button is displayed as well. |
| **Complete these steps from an internet-connected Windows computer.** | | |
| Validate Azure AD and MDM Enrollment | | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Users > All users > Test User1**. 5. Click **Devices**. 6. Confirm that the device is listed there and the following settings are configured:   JOIN TYPE: **Azure AD joined**  MDM: **Microsoft Intune** |
| **Complete these steps from the HYPER-V Host.** | | |
| Revert Virtual Machines | 1. Revert **HYD-CLIENT4** to the latest checkpoint. | |

### Windows Autopilot for White Glove Deployment

Windows Autopilot enables organizations to easily provision new devices – leveraging the preinstalled OEM image and drivers with a simple process that can be performed by the end user to help get their device business-ready.

Windows Autopilot can also provide a **white glove** service that enables partners or IT staff to pre-provision a Windows 10 PC so that it is fully configured and business-ready. From the end user’s perspective, the Windows Autopilot user-driven experience is unchanged, but getting their device to a fully provisioned state is faster.

With **Windows Autopilot for white glove deployment**, the provisioning process is split. The time-consuming portions are performed by IT, partners, or OEMs. The end user simply completes a few necessary settings and policies and they can begin using their device.

Enabled with Microsoft Intune in Windows 10, version 2h1H1 and later, white glove deployment capabilities build on top of existing Windows Autopilot user-driven scenarios, supporting both the user-driven Azure AD join and Hybrid Azure AD join scenarios.

For more information, refer to <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/white-glove>

**Prerequisites:**

1. Windows 10, version 2004 or later is required.
2. An Intune subscription.
3. **Physical devices** that support TPM 2.0 and device attestation; **virtual machines are not supported**. The white glove provisioning process leverages Windows Autopilot self-deploying capabilities, hence the TPM 2.0 requirements.
4. **Physical devices** with Ethernet connectivity; Wi-Fi connectivity is not supported due to the requirement to choose a language, locale, and keyboard to make that Wi-Fi connection; doing that in a pre-provisioning process could prevent the user from choosing their own language, locale, and keyboard when they receive the device.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on a Physical Machine that supports TPM 2.0 and Device Attestation and is installed with Windows 10, version 21H1** | |
| Capture Device ID | 1. Open PowerShell as an administrator. Accept the UAC prompt if required. 2. Run the below commands and press **Y** and **A** wherever prompted. Install-Script –Name Get-WindowsAutoPilotInfo   Set-ExecutionPolicy Unrestricted   1. Change the directory to **C:\Program Files\WindowsPowerShell\Scripts** and run the below command.   **Note:** Ensure that **Windows Remote Management (WS-Management)** service is running on the machine for the script to be executed successfully. .\Get-WindowsAutoPilotInfo.ps1 -ComputerName <ComputerName> –OutputFile C:\Users\<UserName>\Desktop\MyComputers.csv   1. Copy the MyComputers.csv file to the computer that will be used for Microsoft Intune setup. 2. Open Command Prompt as an administrator. Accept the UAC prompt if required. 3. Run the following command after changing the directory to **C:\Windows\System32\Sysprep** SYSPREP\Sysprep.exe /OOBE /SHUTDOWN |
| **Complete these steps from an internet-connected Windows computer.** | |
| Configure AutoPilot White Glove | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to [https://www.portal.azure.com/](https://www.portal.azure.com/en-us/business-store) and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Click **Device enrollment** > **Windows enrollment** > **Devices**. 6. Click **Import,** and select the **MyComputers.csv** file saved from before and click **Import**. 7. Once imported, to speed up the process, click **Sync** and then click **Refresh** until you see the device. 8. Under the **Microsoft Intune** pane, click **Groups > + New group**. 9. Select **Group type – Security**, **Group name – AutoPilot White Glove Devices** and **Membership type – Assigned**. 10. Click **Members**, select the machine where the name equals the serial number of the device. Click **Select**. 11. Click **Create**. 12. On the **Device enrollment** > **Windows enrollment** pane, click **Deployment Profiles** > **+ Create profile**. 13. On the **Basics** tab, in the **Name** box, type **AutoPilot White Glove Test Profile** and click **Next**. 14. On the **Out-of-box experience (OOBE)** tab, in the **Deployment mode** dropdown, select **User-Driven**. 15. In the **Join to Azure AD as** dropdown, select **Azure AD joined**. 16. Select **Hide** for the **Microsoft Software License Terms** option. 17. Select **Hide** for the **Privacy Settings** option. 18. Select **Hide** for the **Hide change account options** option. 19. Select **Standard** for the **User account type** option. 20. Select **Yes** for **Allow White Glove OOBE**. 21. Click **Next**. 22. In the **Assignments** tab, click **+ Select groups to include**, select the **AutoPilot White Glove Devices** group just created and click **Select** and then click **Next**. 23. In the **Review + create** tab, click **Create.** 24. Wait for some time for the device to be showing up in **Assigned devices** under **AutoPilot White Glove Test Profile**. To speed up the process, click **Sync** and then click **Refresh** in the **Device enrollment** > **Windows enrollment** > **Devices** pane, until you see the device there. 25. Click the **Devices** page, and you should be able to see the **PROFILE STATUS** as **Updating** and then further **Assigned**. Wait for a few moments. 26. Select the device imported and click **Assign user**. 27. Type in and select **Test User1** or **TU1@<AzureDomainName>.onmicrosoft.com** and click **Select**. Click **Save**. Wait for a moment while the device is assigned to the user. |
| **Complete these steps on a Physical Machine that supports TPM 2.0 and Device Attestation and is installed with Windows 10, version 21H1** | |
| Technician Flow | 1. Start the machine and once OOBE has started, press the **Windows key five times** to view an additional options dialog. From that screen, choose the **Windows Autopilot provisioning** option and then click **Continue**. 2. On the **Windows Autopilot Configuration** screen, the following information will be displayed about the device: 3. The Autopilot profile assigned to the device - **AutoPilot White Glove Test Profile** 4. The organization name for the device - **<AzureDomainName>.onmicrosoft.com** 5. The user assigned to the device - **TU1@<AzureDomainName>.onmicrosoft.com** 6. A QR code containing a unique identifier for the device, useful to look up the device in Intune to make any configuration changes (example: assigning a user, adding the device to any additional groups needed for app or policy targeting). 7. Validate the information displayed. If any changes are needed, make those and then **Refresh** to re-download the updated Autopilot profile details. 8. Click **Provision** to begin the provisioning process. 9. Once the pre-provisioning process completes successfully, a **green** status screen will be displayed with information about the device, including the same details presented previously (Autopilot profile, organization name, assigned user, QR code), as well as the elapsed time for the pre-provisioning steps. 10. Click **Reseal** to shut the device down. At that point, the device can be shipped to the end user.   **Note:** If the pre-provisioning process fails, a **red** status screen will be displayed with information about the device, including the same details presented previously (Autopilot profile, organization name, assigned user, QR code), as well as the elapsed time for the pre-provisioning steps. **Diagnostic logs** can be gathered from the device, and then it can be **reset** to start the process over again. |
| User Flow | 1. Start the VM and once OOBE has started, in the **Hi Test User1! Welcome to Microsoft Services** pane, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**. 2. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 3. In the **All set!** pane, click **OK**. |
| Validate Azure AD Join and MDM Enrollment | 1. Go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Confirm that **Connected to <CompanyName>’s Azure AD** is displayed and the **Info** button is displayed as well. |
| **Complete these steps from an internet-connected Windows computer.** | |
| Validate Azure AD and MDM Enrollment | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Users > All users > Test User1**. 5. Click **Devices**. 6. Confirm that the device is listed there and the following settings are configured:   JOIN TYPE: **Azure AD joined**  MDM: **Microsoft Intune** |

### AutoPilot for Existing Devices

Modern desktop management with Windows AutoPilot enables you to easily deploy the latest version of Windows 10 to your existing devices. The apps you need for work can be automatically installed. Your work profile is synchronized, so you can resume working right away.

In this section, you will convert a Windows 7 domain-joined computer to Azure Active Directory-joined computer running Windows 10 by using Windows AutoPilot.

**Note:** On **WIN7**, revert to the first checkpoint. Ensure it is in a cleaned state with no incompatible software installed. Software that can conflict can be antivirus or firewall software which should be uninstalled if they exist. Also, during applying the checkpoints back and forth, there is a possibility that the VM loses domain trust relationship. In that case, disjoin and then rejoin the VM to the domain. While doing so, ensure that the VM is cleaned up in AD and ConfigMgr and after the domain-join the VM shows active in both AD and ConfigMgr. Also, to avoid any deployments to be triggered from **CM1** from the previous labs, delete those deployments in **CM1**. If you see **System Center Endpoint Protection** and **Windows Firewall Configuration Provider** at any stage, uninstall both of them.

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | | |
| Configure Enrollment Status Page | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://www.portal.azure.com/> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **All services > search and click Intune > Intune**. 4. Click **Device enrollment > Windows enrollment > Enrollment Status Page**. 5. For the **Default** setting, click **All users and all devices** link and then click **Properties**. 6. Click **Edit** next to **Settings**. 7. For the **Show app and profile installation progress**, select **Yes** and then click **Review + save**. 8. Click **Save**. | |
| **Complete these steps on the DC1 virtual machine.** | | |
| Download .Net Framework 4.8 and Windows Management Framework | 1. Browse to <https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer> and download the **ndp48-web.exe** file to **C:\Packages**. 2. Browse to <https://www.microsoft.com/en-us/download/details.aspx?id=54616> and download the **Win7AndW2K8R2-KB3191566-x64.zip** file to **C:\Packages**. | |
| **Complete these steps on the WIN7 virtual machine.** | | |
| Install .Net Framework 4.8 and Windows Management Framework | 1. Log in to **WIN7** as **CORP\LabAdmin** and browse to **\\DC1\C$\Packages** and copy the **ndp48-web.exe** and **Win7AndW2K8R2-KB3191566-x64.zip** files to the desktop. 2. Right-click **ndp48-web.exe** and click **Run as administrator**. 3. After the extraction completes and the installation wizard starts, select **I have read and accept the license terms** and click **Install**. 4. After the download and installation completes, click **Finish** and then click **Restart Now** to restart **WIN7** and re-log in with the same credentials. 5. Right-click **Win7AndW2K8R2-KB3191566-x64.zip** and click **Extract All...** 6. Click **Extract**. A new window will open up with the extracted files. 7. Right-click **Install-WMF5.1.ps1** and click **Edit | Open**. 8. At the bottom of the Windows PowerShell ISE window, execute the command - **Set-ExecutionPolicy Unrestricted** and accept any prompts. 9. Then press the **Run Script** button to execute the **Install-WMF5.1.ps1** script and accept any prompts. 10. Click **Yes** to install the **Update for Windows (KB3191566)**. 11. Click **I Accept**. 12. Once the installation of the update completes, click **Restart Now** to restart **WIN7** and re-log in with the same credentials. | |
| Create the JSON File | 1. Launch an elevated **Windows PowerShell** command window. 2. Execute the command - **[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12**. 3. Execute the command - **Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force**. 4. Then execute the command - **Install-Module AzureAD -Force**. 5. Then execute the command - **Install-Module WindowsAutopilotIntune -Force**. 6. Then execute the command - **Connect-MSGraph**. **Note:** If you get an error (Stack overflow at line:19) for the first time on the form. Click **OK**, close the form, ignore the error and re-execute the command. 7. On the form, log in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Sign in**. 8. Select **Consent on behalf of your organization** and click **Accept**. 9. Now, execute the command - **Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON**.   **Note:** This is the data from the Autopilot profile created in the previous section and we are not going to make any changes at this moment to the file, however data can be changed as per the table provided here - <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices>   1. Next, execute the command - **Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON | Out-File c:\Windows\AutopilotConfigurationFile.json -Encoding ASCII**. 2. Copy the **AutopilotConfigurationFile.json** to **\\CM1\Packages$\AutopilotConfig** after creating a folder called **AutopilotConfig** in **CM1 - C:\Packages**. | |
| **Complete these steps on the CM1 virtual machine.** | | |
| Create a Package containing the JSON File | 1. In the Configuration Manager Console, browse to **Software Library | Overview | Application Management | Packages**. 2. On the ribbon bar, click **Create Package**. 3. On the Package screen, enter the following and click **Next**:   Name: **Autopilot for Existing Devices Config**  This package contains source files: **Selected**  Source folder: **\\CM1\Packages$\AutopilotConfig**   1. On the Program Type screen, select **Do not create a program** and click **Next**. 2. On the Summary screen, click **Next**. 3. On the Completion screen, click **Close**. | |
| Create a Target Collection | | 1. Browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **Autopilot for Existing Devices Collection**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule | Direct Rule** and click **Next** on the Welcome page. 2. In the Search for Resources page, in the Value, enter **WIN7** and then click **Next**. 3. In the Select Resources page, select **WIN7** and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. 6. Back on the Membership Rules page, click **Next**. 7. On the Summary page, click **Next**. 8. On the Completion page, click **Close**. 9. Ensure that the **WIN7** machine is present in the **Autopilot for Existing Devices** Collection. |
| Create an Autopilot for Existing Devices Task Sequence | | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Click **Create Task Sequence** from the ribbon bar. 3. On the Create New Task Sequence page, select **Install an existing image package** and click **Next**. 4. On the Task Sequence Information page, enter **Autopilot for Existing Devices** for the Task sequence name. 5. Click **Browse...**next to Boot image, select **MDT Boot image (x64) en-us** and then click **OK**. 6. Click **Next**. 7. On the Install Windows page, click **Browse...**next to Image package. Select **Windows 10 - x64 en-US** and then click **OK**. The Image index will be auto populated with **1 - ICS002DDrive**. 8. On the Install Windows page, ensure that **Partition and format the target computer before installing the operating system** is selected and uncheck **Configure task sequence for use with BitLocker**. 9. On the Install Windows page, keep the rest as default settings and click **Next**. 10. On the Configure Network page, select **Join a workgroup** and enter the name as **WORKGROUP**. Click **Next**. 11. On the Install Configuration Manager page, click **Next**. 12. On the State Migration page, uncheck **Capture user settings and files**, **Capture network settings** and **Capture Microsoft Windows settings**. Click **Next**. 13. On the Include Updates page, keep the default settings and click **Next**. 14. On the Install Applications page, keep the default settings and click **Next**. 15. On the Summary page, click **Next**. 16. On the Completion page, click **Close**. 17. Right-click **Autopilot for Existing Devices** task sequence and click **Edit**. 18. Under the **Install Operating System** group, click the **Apply Windows Settings** step. 19. Click **Add | New Group**. 20. Change the group Name from **New Group** to **Autopilot for Existing Devices Config**. 21. Now click **Add | General | Run Command Line**. Ensure that this step is under the **Autopilot for Existing Devices Config** group. 22. Change the Name to **Apply Autopilot for Existing Devices Config File** and enter the following Command line in the Command line text box - **cmd.exe /c xcopy AutopilotConfigurationFile.json %OSDTargetSystemDrive%\windows\provisioning\Autopilot\ /c**. Click **Apply**. 23. In the Apply Autopilot for Existing Devices Config File step, select **Package** and click **Browse...** 24. Select **Autopilot for Existing Devices Config** package and then click **OK**. 25. Under the Setup Operating System group, click the **Setup Windows and Configuration Manager** step. 26. Click **Add | New Group**. 27. Change the group Name from **New Group** to **Prepare Device for Autopilot**. Ensure it is the very last item in the task sequence at the moment. 28. Now click **Add | Images | Prepare ConfigMgr Client for Capture**. 29. Once again click **Add | Images | Prepare Windows for Capture**. 30. Do not select any of the checkboxes under **Prepare Windows for Capture** step and then finally click **Apply | OK**. |
| Deploy Content to Distribution Point | | 1. Right-click **Autopilot for Existing Devices** task sequence and click **Distribute Content**. 2. On the General page, click **Next**. 3. On the Content page, click **Next**. 4. On the Content Distribution page, click **Add | Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 5. On the Summary page, click **Next**. 6. On the Completion page, click **Close**. Ensure that all content has been distributed from the **Monitoring | Overview | Distribution Status | Content Status**. |
| Deploy the Autopilot for Existing Devices Task Sequence | | 1. Right-click **Autopilot for Existing Devices** task sequence and click **Deploy**. 2. On the General page, click **Browse...**, click **OK** on the prompt, select **Autopilot for Existing Devices Collection**, click **OK** and then click **Next**. 3. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Only Configuration Manager Clients** is selected under Make available to the following. Click **Next**. 4. On the Scheduling page, click **Next**. 5. On the User Experience page, click **Next**. 6. On the Alerts page, click **Next**. 7. On the Distribution Points page, click **Next**. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. |
| **Complete these steps on the WIN7 virtual machine.** | | |
| Execute the Autopilot for Existing Devices Task Sequence | | 1. Click **Start | Control Panel**. 2. Click **System and Security | Configuration Manager**. 3. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 4. Click **Run Now** and then click **OK**. 5. Click the **notification** or open the **Software Center**. 6. Under Operating Systems select **Autopilot for Existing Devices** and then click **Install**. 7. Click **Install** again on the prompt. 8. The Task Sequence will download content, reboot, format the drives and install Windows 10. The virtual machine will then proceed to be prepared for Autopilot. Once the task sequence has completed the virtual machine will boot into OOBE and provide an Autopilot experience. 9. Once OOBE has started, in the Let’s start with region. Is this right? pane, select **United States** then click **Yes**. 10. On the Account screen, enter the username: **TU2@<AzureDomainName>.onmicrosoft.com**, then click **Next**. 11. Enter the **password** for **TU2@<AzureDomainName>.onmicrosoft.com** and then click **Next**. 12. Notice the Setting up your device for work screen. This is coming from the Enrollment Status Page. 13. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 14. In the **All set!** pane, click **OK**. 15. You will be logged in to the desktop. |
|  | |  |

## Deploy and manage the new Microsoft Edge

The new Microsoft Edge enhances and extends the browser experience. It runs on Windows, macOS, iOS and Android devices. In this section, we will perform the following core scenarios:

* Deploy and Update Edge
* Deploy Edge using Configuration Manager
* Deploy Edge Updates using Configuration Manager
* Configure and Deploy Edge Policies using On-Premises Method
* Deploy Edge using Intune
* Configure and Deploy Edge Policies using Intune
* IE Mode
* Configure and Deploy IE Mode using On-Premises Method
* Configure and Deploy IE Mode using Intune
* Application Guard
* Setup Enterprise New Tab Page
* Configure and Deploy Enterprise New Tab using On-Premises Method
* Configure and Deploy Enterprise New Tab using Intune
* Access Microsoft Edge Legacy after installing the new version of Microsoft Edge (Side-by-Side)

### Deploy and Update Edge

In this section, we will perform the following scenarios:

* Deploy Edge using Configuration Manager
* Deploy Edge Updates using Configuration Manager
* Configure and Deploy Edge Policies using On-Premises Method
* Deploy Edge using Intune or Microsoft Endpoint Manager (MEM)
* Configure and Deploy Edge Policies using Intune

#### Deploy Edge using Configuration Manager

In this section, we will deploy Edge using Configuration Manager (MECM), which is the on-premises Method.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Configure Execution Policy | 1. Launch an elevated PowerShell window. 2. Run the command **Get-ExecutionPolicy**. If the result is **Restricted**, then run the command **Set-ExecutionPolicy Unrestricted** and accept all the prompts. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Folder | 1. Open **File Explorer** and navigate to **C:\Packages** and create a folder called **Edge**. |
| Create a Device Collection | 1. Launch the Configuration Manager console and navigate to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. On the General page, specify the following and click **Next**:   Name: **Edge Clients**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule > Direct Rule**. On the Welcome page click **Next**. On the Search for Resources page, enter **%CLIENT1%** next to Value and click **Next**. On the Select Resources page, select **CLIENT1** and click **Next**. On the Summary page, click **Next**. On the Completion page, click **Close**. 2. Back on the Membership Rules page, click **Next**. 3. On the Summary page, click **Next**. 4. On the Completion page, click **Close**. 5. Ensure that the **Edge Clients** collection has **CLIENT1** in it. |
| Create the Microsoft Edge Application and Deployment | 1. Navigate to **Software Library > Microsoft Edge Management**. 2. Right-click **Microsoft Edge Management** and select **Create Microsoft Edge Application**. 3. In the Application Settings page, specify a Name - **Edge App** and Content Location - **\\CM1\Packages$\Edge** and then click **Next**. 4. In the Specify settings for Microsoft Edge client page, for Channel select **Stable** and select **Specific Version**. In the Specific Version, select the **lowest possible version as we will be updating it later**. Click **Next**.   **Note:** Make a note of the lowest and latest possible versions from the drop-down list.   1. On the Deployment page, select **Yes** and click **Next**. 2. On the General page, select **Edge Clients** next to Collection which comes under the category of **Device Collections** and click **Next**. 3. On the Content page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 4. On the Deployment Settings page, ensure **Install** is selected next to Action and select **Available** next to Purpose. Click **Next**. 5. On the Scheduling page, click **Next**. 6. On the User Experience page, select **Display in Software Center and show all notifications** next to User notifications and click **Next**. 7. On the Alerts page, click **Next**. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. Click the **Actions** tab and select **Machine Policy Retrieval & Evaluation Cycle** and **Application Deployment Evaluation Cycle** and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process. 3. As soon as the notification appears, click on the **notification or launch Software Center**. 4. Select **Edge App** under Applications and click **Install**. 5. Once the installation is completed, notice the **new Microsoft Edge icon on the desktop**. |

#### Deploy Edge Updates using Configuration Manager

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Folder | 1. Open **File Explorer** and navigate to **C:\Packages** and create a folder called **EdgeUpdates**. |
| Configure Software Update Point | 1. Launch the Configuration Manager console and navigate to **Administration > Site Configuration > Sites**. 2. Right-click the site and select **Configure Site Components > Software Update Point**. 3. Click the **Classifications** tab, **uncheck all the boxes** and only select **Updates**. 4. Click the **Products** tab, **uncheck all the boxes** and only select **Microsoft Edge** under **Windows**. 5. Click the **Languages** tab, ensure and only select **English**. If other languages are selected, deselect them all. Click **Apply** and **OK**. 6. Navigate to **Software Library > Microsoft Edge Management > All Microsoft Edge Updates** and click **Synchronize Software Updates** and click **Yes**.   **Note:** Synchronization can take up to an hour or so.   1. Once the synchronization has completed, refresh the **All Microsoft Edge Updates** to view the metadata. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Refresh Policies | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. Click the **Actions** tab and select **all the actions** one by one and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process so that update shows in **Required** state. It could take up to an hour or so for the update to be detected in **Required** state. |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure and Deploy Microsoft Edge Updates | 1. In the **All Microsoft Edge Updates** pane, in order to view the Title of the update, right-click in the **heading panel** and enable **Title**. 2. Sort out the updates based on **Stable**, **Dev** and **Beta** by clicking on the **Title header**. 3. Since you took a note of the lowest and latest possible versions from the drop-down list previously, look for the **latest Stable version** in the list and select both the **x86** and **x64** of that version (Ctrl and select to select multiple versions). 4. From the ribbon bar, click **Deploy**. 5. On the General page, for the Deployment Name, enter **Edge Stable Updates**, for the Collection, select **Edge Clients** and then click **Next**. 6. On the Deployment Settings page, keep the defaults and click **Next**. 7. On the Scheduling page, select **As soon as possible** under Installation deadline and click **Next**. 8. On the User Experience page, keep the defaults and click **Next**. 9. On the Alerts page, keep the defaults and click **Next**. 10. On the Deployment Package page, select **Create a new deployment package**, enter the Name - **Edge Stable Updates**, enter the Package source - **\\CM1\Packages$\EdgeUpdates** and then click **Next**. 11. On the Distribution Points page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 12. On the Download Location page, keep the defaults and click **Next**. 13. On the Language Selection page, select **Windows Update** and click **Next**. 14. On the Download Settings page, select **Download software updates from distribution point and install** under Deployment options and then click **Next**. 15. On the Summary page, review and click **Next**. 16. On the Completion page, click **Close**. 17. Navigate to **Software Library > Software Updates > Software Update Groups**, select the **software update group** and click **Run Summarization** few times and click **Refresh** few times from the ribbon bar to ensure that the client machine shows into **non-compliance**, which means that the machine needs one of the updates in the software update group. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge Updates | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. Click the **Actions** tab and select **all the actions** one by one and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process. 3. As soon as the notification appears, click on the **notification or launch Software Center**. 4. Notice that the update gets **downloaded and installed**. 5. Once the installation is completed, launch **Control Panel > Programs > Programs and Features** and notice that the **Microsoft Edge version has been updated**. |

#### Configure and Deploy Edge Policies using On-Premises Method

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Download and Install Administrative Templates for Microsoft Edge | 1. Open Internet Explorer and browse to <https://aka.ms/EdgeEnterprise> to download the administrative templates for Microsoft Edge. Select the **latest Channel/Version and Build**, select the **Platform Windows 64-bit** and then click **GET POLICY FILES**. 2. Click **Accept and download**. Save the **MicrosoftEdgePolicyTemplates.zip** file to the **desktop** and click **Close** and close Internet Explorer. 3. Right-click **MicrosoftEdgePolicyTemplates.zip** and click **Extract All**. 4. Click **Extract**. 5. On the opened folder where the content has been extracted to, navigate to **windows > admx**. 6. Scroll down and copy the **msedge.admx** and **msedgeupdate.admx** files to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. Click **Continue** on the prompt. 7. Now, navigate to **windows > admx > en-US** and copy the **msedge.adml** and **msedgeupdate.adml** files to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions\en-US**. Click **Continue** on the prompt. |
| Configure and Deploy Microsoft Edge Policies | 1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here...** 3. Specify the Name - **Microsoft Edge Policies** and click **OK**. 4. Right-click **Microsoft Edge Policies** and click **Edit...** 5. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Default search provider**. 6. Double-click **Enable the default search provider**, select **Enabled**, click **Apply** and **OK**. 7. Double-click **Default search provider name**, select **Enabled**, under Default search provider name, enter **Google** and then click **Apply** and **OK**. 8. Close all the windows. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Verify Microsoft Edge Policies | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. Launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter. 4. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**. |

#### Deploy Edge using Intune

In this section, we will deploy Edge using Intune, which is the Cloud solution.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Configure Execution Policy | 1. Launch an elevated PowerShell window. 2. Run the command **Get-ExecutionPolicy**. If the result is **Restricted**, then run the command **Set-ExecutionPolicy Unrestricted** and accept all the prompts. |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create a Security Group | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **Azure Active Directory** and then click **Groups**. 3. Under All groups, click **+ New group**. 4. Enter the following and then click **Create**:   Group type: **Security**  Group name: **EdgePoC**  Membership type: **Assigned**  Members: **CLIENT3** |
| Create the Microsoft Edge App and Assignment | 1. Navigate to <https://devicemanagement.microsoft.com> which is the **Microsoft Endpoint Manager Admin Center** and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. Select **Apps > All apps > + Add**. 3. Under Microsoft Edge, version 77 and later, select **Windows 10** and then click **Select**. 4. On the App information tab, keep all defaults and click **Next**. 5. On the App settings tab, select **Stable** next to Channel. Note the new Logo. Click **Next**. 6. On the Assignments tab, under Required, click **+ Add group**. Select **EdgePoC** and then click **Select**. Click **Next**. 7. On the Review + create tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. In few minutes, notice a **notification** from Intune stating that **Microsoft Edge is being downloaded and installed** and also notice the **new Microsoft Edge icon on the desktop**. **The latest version of Microsoft Edge will be installed from the Stable channel by default.** |

#### Configure and Deploy Edge Policies using Intune

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Configure and Deploy Microsoft Edge Policies | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **+ Create profile**. 5. Select the following and click **Create**:   Platform: **Windows 10 and later**  Profile: **Administrative Templates**   1. On the Basics tab, enter **Microsoft Edge Policies** next to **Name** and click **Next**. 2. On the Configuration settings tab, navigate to **Computer Configuration > Microsoft Edge > Default search provider** and click the policy **Enable the default search provider**. Select **Enabled** and click **OK**. 3. Now click the policy - **Default search provider name**. Select **Enabled** and under Default search provider name, enter **Google**. Click **OK**. 4. On the Configuration settings tab. Click **Next**. 5. On the Scopes tags tab, click **Next**. 6. On the Assignments tab, click **Select groups to include**, select **EdgePoC** and click **Select**. Click **Next**. 7. On the Review + create tab, review the settings and click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Microsoft Edge Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. Once the sync has completed, after sometime, launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter. 5. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**. |

### IE Mode

In this section, we will perform the following scenarios:

* Configure and Deploy IE Mode using On-Premises Method
* Configure and Deploy IE Mode using Intune

#### Configure and Deploy IE Mode using On-Premises Method

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the APP1 virtual machine.** | |
| Create a Shared Folder (EMEI) with Full Permissions | 1. Open File Explorer and browse to **C:\**. 2. Create a new folder named **EMEI**. 3. Right-clickon **EMEI** and select **Properties**. 4. In the EMEI Properties window, go to the **Sharing** tab. 5. On the Sharing tab, click **Advanced Sharing**. 6. On the Advanced Sharing window, select **Share this folder** then click on **Permissions**. 7. On the Permissions for EMEI window, under **Allow** select **Full Control** then click **Apply** and **OK**. 8. On the Advanced Sharing window, click **Apply** and **OK**. 9. On the EMEI Properties window, click **Close**. |
| Configure Test Website | 1. On the taskbar, open **File Explorer** and browse to **C:\Packages\Sources**. 2. Copy the **ContosoLearning** folder to **C:\inetpub\wwwroot**. Accept the prompt. 3. On the Start menu, open **Internet Information Services (IIS) Manager**. 4. Under the **Connections** pane, browse to **APP1 (Corp\LabAdmin) > Sites > Default Web Site > ContosoLearning**. 5. Right-click on **ContosoLearning** and select **Convert to Application**. 6. On the Add Application window, click **OK**. 7. On **ContosoLearning**, under the **Actions** pane select **Advanced Settings.** 8. On the Advanced Settings window, select **Application Pool** and click on the **ellipses (…)**. 9. On the Select Application Pool window, set the **Application pool** to **.NET v2.0** then click **OK**. 10. On the Advanced Settings window, click **OK**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Pin Internet Explorer on the Taskbar | 1. On the **Start** Menu, search for **Internet Explorer**. 2. Right-click on **Internet Explorer** and select **Pin to taskbar**. |
| Download Enterprise Mode Site List Manager | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49974>   1. From the website, click **Download**. 2. Save **EMIESiteListManager.msi** to **C:\Packages** after creating a folder called **Packages** in **C:\**. |
| Install Enterprise Mode Site List Manager | 1. On the taskbar, open **File Explorer** and browse to **C:\Packages**. 2. Double-click on **EMIESiteListManager.msi**. 3. On the Welcome page, click **Next**. 4. On the End-User License Agreement page, select **I accept the terms in the License Agreement** and then click **Next**. 5. On the Destination Folder page, click **Next**. 6. On the Ready to Install page, click **Install**. Accept the UAC prompt if required. 7. Once complete, click **Finish**. |
| Create a Site List | 1. From the desktop icon, open the **Enterprise Mode Site List Manager**. 2. On the Enterprise Mode Site List Manager for v.2 schema window, click **Add**. 3. On the Add new website window, under **URL** enter **app1/ContosoLearning** and select **IE8 Document Mode** next to **Compat Mode** and then click **Save**. 4. Click on **File >** **Save to XML**. 5. **Save** the file to **\\APP1\EMEI** as **EMEISiteList.xml**. |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure and Deploy IE Mode Policies | 1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **Microsoft Edge Policies** and click **Edit...** 3. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge**. 4. Look for the policy - **Configure Internet Explorer integration** and double-click it. 5. Select **Enabled** and under Options, select **Internet Explorer mode**. Click **Apply** and **OK**. 6. Now look for the policy - **Configure the Enterprise Mode Site List** and double-click it. 7. Select **Enabled** and under Options, enter **\\APP1\EMEI\EMEISiteList.xml**. Click **Apply** and **OK**. 8. Close all the windows. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Verify IE Mode Policies | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. First launch **IE11** and in the address bar type **http://app1/ContosoLearning** and press enter. 4. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 5. Now launch the new **Microsoft Edge** and in the address bar type **http://app1/ContosoLearning** and press enter. 6. Notice that the new **Microsoft Edge opens the website in Internet Explorer mode**. You can notice an **icon of Internet Explorer in the address bar** on which when you hover you mouse, it displays **Internet Explorer mode**. Also notice that you will **not see the warning**. |

#### Configure and Deploy IE Mode using Intune

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the APP1 virtual machine.** | |
| Host the EMEISiteList.xml in Contoso Learning | 1. Navigate to **C:\EMEI** and copy the **EMEISiteList.xml** file. 2. Right-click **Start > Run, type inetmgr** and press enter. 3. Navigate to **APP1 (CORP\LabAdmin) > Sites > Default Web Site > Contoso Learning**. 4. Right-click **Contoso Learning** and click **Explore**. 5. Paste the **EMEISiteList.xml** in this location along with the rest of the files. 6. Open **Internet Explorer** and ensure that you are able to access **http://APP1/ContosoLearning/EMEISiteList.xml**. |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Configure and Deploy IE Mode Policies | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **Microsoft Edge Policies** and click **Properties**. 5. Click **Edit** next to **Configuration settings**. 6. Navigate to **Computer Configuration > Microsoft Edge** and search for the policy - **Configure Internet Explorer integration** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under Configure Internet Explorer integration, select **Internet Explorer mode** and click **OK**. 7. Now search for the policy - **Configure the Enterprise Mode Site List** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under Configure the Enterprise Mode Site List, enter **http://APP1/ContosoLearning/EMEISiteList.xml** and click **OK**. 8. Click **Review + save** at the bottom and then click **Save** again. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify IE Mode Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. First launch **IE11** and in the address bar type **http://app1/ContosoLearning** and press enter. 5. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 6. Once the sync has completed, after sometime, launch the new **Microsoft Edge**. 7. In the address bar type **http://app1/ContosoLearning** and press enter. 8. Notice that the new **Microsoft Edge opens the website in Internet Explorer mode**. You can notice an **icon of Internet Explorer in the address bar** on which when you hover you mouse, it displays **Internet Explorer mode**. Also notice that you will **not see the warning**. |

### Application Guard

First perform the prerequisites in **Section 4.2 - Security and Compliance (Steps 1-20)**, then perform **Section 4.2.5 - Windows Defender Application Guard**.

### Setup Enterprise New Tab Page

In this section, we will perform the following scenarios:

* Configure and Deploy Enterprise New Tab using On-Premises Method
* Configure and Deploy Enterprise New Tab using Intune

#### Configure and Deploy Enterprise New Tab using On-Premises Method

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure and Deploy Enterprise New Tab Policies | 1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **Microsoft Edge Policies** and click **Edit...** 3. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Startup, home page and new tab page**. 4. Look for the policy - **Configure the new tab page URL** and double-click it. 5. Select **Enabled** and under Options, enter **http://www.microsoft.com**. Click **Apply** and **OK**. 6. Now look for the policy - **Action to take on startup** and double-click it. 7. Select **Enabled** and under Options, under Action to take on startup, select **Open a list of URLs**. Click **Apply** and **OK**. 8. Now look for the policy - **Sites to open when the browser starts** and double-click it. 9. Select **Enabled** and under Options, click **Show...** and enter **http://www.bing.com** and **http://www.google.com** and then click **OK**. Click **Apply** and **OK**. 10. Now look for the policy - **Show Home button on toolbar** and double-click it. 11. Select **Enabled**. Click **Apply** and **OK**. 12. Close all the windows. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Verify Enterprise New Tab Policies | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. Now launch the new **Microsoft Edge**. First notice the **home button** at the **toolbar**. Then notice that **Bing** and **Google** websites were opened at the launch of the browser in **2 separate tabs**. 4. Now start a **new tab**. Notice that **Microsoft's** website opens up. |

#### Configure and Deploy Enterprise New Tab using Intune

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Configure and Deploy Enterprise New Tab Policies | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **Microsoft Edge Policies** and click **Properties**. 5. Click **Edit** next to **Configuration settings**. 6. Navigate to **Computer Configuration > Microsoft Edge > Startup, home page and new tab page**. Search for the policy - **Configure the new tab page URL** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the New tab page URL, enter **http://www.microsoft.com** and click **OK**. 7. Now search for the policy - **Action to take on startup** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the Action to take on startup, select **Open a list of URLs** and click **OK**. 8. Now search for the policy - **Sites to open when the browser starts** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the Sites to open when the browser starts, enter **http://www.bing.com** and **http://www.google.com** and click **OK**. 9. Now search for the policy - **Show Home button on toolbar** and click the policy from the search results which has the **Setting type Device**. Select **Enabled** and click **OK**. 10. Click **Review + save** at the bottom and then click **Save** again. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Enterprise New Tab Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. Once the sync has completed, after sometime, launch the new **Microsoft Edge**. 5. First notice the **home button** at the **toolbar**. Then notice that **Bing** and **Google** websites were opened at the launch of the browser in **2 separate tabs**. 6. Now start a **new tab**. Notice that **Microsoft's** website opens up. |

### Access Microsoft Edge Legacy after installing the new version of Microsoft Edge (Side-by-Side)

In this section, we will access Microsoft Edge Legacy after installing the new version of Microsoft Edge.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Configure Execution Policy | 1. Launch an elevated PowerShell window. 2. Run the command **Get-ExecutionPolicy**. If the result is **Restricted**, then run the command **Set-ExecutionPolicy Unrestricted** and accept all the prompts. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Device Collection | 1. Launch the Configuration Manager console and navigate to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. On the General page, specify the following and click **Next**:   Name: **Edge Clients (Side-by-Side)**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule > Direct Rule**. On the Welcome page click **Next**. On the Search for Resources page, enter **%CLIENT2%** next to Value and click **Next**. On the Select Resources page, select **CLIENT2** and click **Next**. On the Summary page, click **Next**. On the Completion page, click **Close**. 2. Back on the Membership Rules page, click **Next**. 3. On the Summary page, click **Next**. 4. On the Completion page, click **Close**. 5. Ensure that the **Edge Clients (Side-by-Side)** collection has **CLIENT2** in it. |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure and Deploy the Side-by-Side Browser Experience Policy | 1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **Microsoft Edge Policies** and click **Edit...** 3. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge Update > Applications**. 4. Look for the policy – **Allow Microsoft Edge Side by Side browser experience** and double-click it. 5. Select **Enabled**. Click **Apply** and **OK**. 6. Close all the windows. |
| **Complete these steps on the CM1 virtual machine.** | |
| Deploy the Microsoft Edge Application previously created to the New Collection | 1. Navigate to **Software Library > Application Management > Applications**. 2. Right-click **Edge App** and click **Deploy**. 3. On the General page, select **Edge Clients (Side-by-Side)** next to Collection which comes under the category of **Device Collections** and click **Next**. 4. On the Content page, click **Next**. 5. On the Deployment Settings page, ensure **Install** is selected next to Action and select **Available** next to Purpose. Click **Next**. 6. On the Scheduling page, click **Next**. 7. On the User Experience page, select **Display in Software Center and show all notifications** next to User notifications and click **Next**. 8. On the Alerts page, click **Next**. 9. On the Summary page, click **Next**. 10. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge (Side-by-Side) | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 4. Click the **Actions** tab and select **Machine Policy Retrieval & Evaluation Cycle** and **Application Deployment Evaluation Cycle** and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process. 5. As soon as the notification appears, click on the **notification or launch Software Center**. 6. Select **Edge App** under Applications and click **Install**. 7. Once the installation is completed, notice the **new Microsoft Edge icon on the desktop along with the old Microsoft Edge**. |

# Deploy Microsoft 365 Apps for enterprise

Microsoft 365 Apps for enterprise is the modern client suite with Microsoft 365. The suite is like other versions of Office but there are differences:

* Licensing
* Deployment
* Updates (Channel Management)

Further information on the similarities and differences are in the [About Microsoft 365 Apps in the enterprise](https://support.office.com/en-us/article/About-Office-365-ProPlus-in-the-enterprise-9f11214c-911d-4e3c-9993-a566f12b1a68?ui=en-US&rs=en-US&ad=US)

Microsoft 365 Apps for enterprise can be deployed in 3 scenarios:

* Enterprise Managed
* Locally Managed
* Cloud Managed

Further information on the 3 scenarios are in the [Plan your enterprise deployment of Microsoft 365 Apps](https://support.office.com/en-us/article/Best-practices-Recommended-deployment-scenarios-4d4ff951-ee72-4763-806a-deeb384a369b?ui=en-US&rs=en-US&ad=US)

Microsoft 365 Apps for enterprise is updated leveraging Channels. The 3 channels are:

* Current
* Monthly Enterprise
* Semi-Annual Enterprise

Further information on Microsoft 365 Apps Channels are in the [Overview of update channels for Microsoft 365 Apps](https://support.office.com/en-us/article/Overview-of-update-channels-for-Office-365-ProPlus-9ccf0f13-28ff-4975-9bd2-7e4ea2fefef4?ui=en-US&rs=en-US&ad=US).

**Note:** If there are any 32-bit Office versions installed from the previous sections, uninstalled them from VM’s that are going to be used in this section, as we are now going to focus on 64-bit Office versions and both 32-bit and 64-bit Office versions have a conflict.

**Note:** For more information on the Office Customization Tool, refer to <https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-customization-tool-for-click-to-run>

## Cloud Managed Deployment

In this activity, deploy Microsoft 365 Apps for enterprise from the Content Delivery Network (CDN) using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Download Office Deployment Tool | 1. Logon as corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. The Sample Configurations for all Office Applications – Current Channel from the <https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options> can be referenced. 2. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 8. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Deploy Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. |
| Update Microsoft 365 Apps | 1. Click **Start**. 2. Select **Word**. 3. Click **Blank document**. 4. Click **File**. 5. Click **Account**. 6. Click **Update Options**. 7. Click **Update Now**.   **Note:** Microsoft 365 Apps for enterprise will download the updates and apply the updates from the CDN.   1. Click **Continue** when prompted to close the applications requiring updates.   **Note:** Microsoft 365 Apps for enterprise only requires the applications being updated to be closed and will be re-launched once the update is done.   1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column record the version number of the current month. 3. Click **File**. 4. Click **Account**. 5. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 6. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update Channel**, select the **Version** and **Build** that is currently installed. 3. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 6. Save the file to **C:\ODT**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /configure removeaccess.xml**. 9. Press Enter. 10. Office will begin the installation. 11. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings   **Note:** If creating a Language, set the first language to the client’s culture language. If the first language does not match the client’s culture set, then the chosen language will be the Shell UI language**.**   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\ODT**. 6. Back in CMD, type **setup.exe /configure addspanish.xml**. 7. Press Enter. 8. Office will begin the installation. 9. Click **Close**. 10. Type **Control Panel** inthe “Type here to search” and press Enter. 11. Click on **Programs**. 12. Click on **Programs and Features**. 13. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

## Locally Managed Deployment

In this activity, you will deploy Microsoft 365 Apps for enterprise from a local file share using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Create a File Share for Microsoft 365 Apps | 1. Logon as corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\Packages** and create a folder named **MC**. The **Packages** folder must be created in advance in case it is not created. 3. Right-Click on the **MC** folder and select **Give access to**. 4. Select **“Specific people…”**. 5. Select **Everyone** from the drop down. 6. Click **Add**. 7. Set the Permission Level for Everyone to **Read/Write**. 8. Click **Share**. 9. Record the Share Path. 10. Click **Done**. |
| Download Office Deployment Tool | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\Packages\MC**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\Packages\MC** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. The Sample Configurations for all Office Applications – Current Channel from the <https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options> can be referenced. 2. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT2\MC** and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 8. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\Packages\MC**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Download Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\Packages\MC**. 5. Type **setup.exe /download newconfiguration.xml**. 6. Press Enter. Office will begin the download. |
| Deploy Microsoft 365 Apps (Offline from a Local Share) | 1. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 2. Press Enter. 3. Office will begin the installation. Click **Close**. |
| Update Microsoft 365 Apps (Offline from a Local Share) | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column, record the version number of the current month.   **Note:** Unlike Cloud Managed, the monthly build of Microsoft 365 Apps needs to be downloaded to the local file share.   1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 3. Under **Update and upgrade**, under **Update and upgrade options**, select **Local source** and specify the **Source path** as **\\CLIENT2\MC**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 6. Save the file to **C:\Packages\MC**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /download update.xml**. 9. Press Enter. Office will begin the download. 10. Back in CMD, type **setup.exe /configure update.xml**. 11. Press Enter. 12. Office will begin the installation. Click **Close**. 13. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 14. In the **Current Channel** Column, record the version number of the current month. 15. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 16. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 7. Back in CMD, type **setup.exe /configure removeaccess.xml**. 8. Press Enter. 9. Office will begin the installation. 10. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps (Offline from a Local Share) | 1. Go back to the already opened https://config.office.com/deploymentsettings   **Note:** If creating a Language, set the first language to the client’s culture language. If the first language does not match the client’s culture set, then the chosen language will be the Shell UI language.   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. Back in CMD, type **setup.exe /download addspanish.xml**. 7. Press Enter. Office will begin the download. 8. Back in CMD, type **setup.exe /configure addspanish.xml**. 9. Office will begin the installation. 10. Click **Close**. 11. Type **Control Panel** inthe “Type here to search” and press Enter. 12. Click on **Programs**. 13. Click on **Programs and Features**. 14. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

## Microsoft 365 Apps for enterprise Deployment on Non-AD Joined Devices

In this activity, you will deploy Microsoft 365 Apps for enterprise on a Non-AD Joined Device (**CLIENT4**) using both methods – Cloud Managed and Locally Managed. You will use a combination of Office Customization Tool (OCT) and Office Deployment Tool (ODT) to create the configuration XML and perform activities like deployment of Microsoft 365 Apps, update/upgrade Microsoft 365 Apps, remove an application, add a language and remove prior MSI versions of Microsoft 365 Apps.

**Cloud Managed Deployment**

In this activity, deploy Microsoft 365 Apps from the Content Delivery Network (CDN) using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT4 virtual machine.** | |
| Download Office Deployment Tool | 1. Logon as .\Administrator. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. The Sample Configurations for all Office Applications – Current Channel from the <https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options> can be referenced. 2. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 8. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Deploy Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. |
| Update Microsoft 365 Apps | 1. Click **Start**. 2. Select **Word**. 3. Click **Blank document**. 4. Click **File**. 5. Click **Account**. 6. Click **Update Options**. 7. Click **Update Now**.   **Note:** Microsoft 365 Apps will download the updates and apply the updates from the CDN.   1. Click **Continue** when prompted to close the applications requiring updates.   **Note:** Microsoft 365 Apps only requires the applications being updated to be closed and will be re-launched once the update is done.   1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column record the version number of the current month. 3. Click **File**. 4. Click **Account**. 5. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 6. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is currently installed. 3. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 6. Save the file to **C:\ODT**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /configure removeaccess.xml**. 9. Press Enter. 10. Office will begin the installation. 11. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings   **Note:** If creating a Language, set the first language to the client’s culture language. If the first language does not match the client’s culture set, then the chosen language will be the Shell UI language**.**   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\ODT**. 6. Back in CMD, type **setup.exe /configure addspanish.xml**. 7. Press Enter. 8. Office will begin the installation. 9. Click **Close**. 10. Type **Control Panel** inthe “Type here to search” and press Enter. 11. Click on **Programs**. 12. Click on **Programs and Features**. 13. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

**Locally Managed Deployment**

In this activity, you will deploy Microsoft 365 Apps for enterprise from a local file share using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT4 virtual machine.** | |
| Create a File Share for Microsoft 365 Apps | 1. Logon as .\Administrator. 2. On the taskbar, open File Explorer and browse to **C:\Packages** and create a folder named **MC**. The **Packages** folder must be created in advance in case it is not created. 3. Right-Click on the **MC** folder and select **Give access to**. 4. Select **“Specific people…”**. 5. Select **Everyone** from the drop down. 6. Click **Add**. 7. Set the Permission Level for Everyone to **Read/Write**. 8. Click **Share**. 9. Record the Share Path. 10. Click **Done**. |
| Download Office Deployment Tool | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\Packages\MC**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\Packages\MC** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. The Sample Configurations for all Office Applications – Current Channel from the <https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options> can be referenced. 2. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT4\MC** and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 8. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\Packages\MC**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Download Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\Packages\MC**. 5. Type **setup.exe /download newconfiguration.xml**. 6. Press Enter. Office will begin the download. |
| Deploy Microsoft 365 Apps (Offline from a Local Share) | 1. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 2. Press Enter. 3. Office will begin the installation. Click **Close**. |
| Update Microsoft 365 Apps (Offline from a Local Share) | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column, record the version number of the current month.   **Note:** Unlike Cloud Managed, each month, the monthly build of Microsoft 365 Apps needs to be downloaded to the local file share.   1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 3. Under **Update and upgrade**, under **Update and upgrade** options, select **Local source** and specify the **Source path** as **\\CLIENT4\MC**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 6. Save the file to **C:\Packages\MC**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /download update.xml**. 9. Press Enter. Office will begin the download. 10. Back in CMD, type **setup.exe /configure update.xml**. 11. Press Enter. 12. Office will begin the installation. Click **Close**. 13. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 14. In the **Current Channel** Column, record the version number of the current month. 15. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 16. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 7. Back in CMD, type **setup.exe /configure removeaccess.xml**. 8. Press Enter. 9. Office will begin the installation. 10. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps (Offline from a Local Share) | 1. Go back to the already opened https://config.office.com/deploymentsettings   **Note:** If creating a Language, set the first language to the client’s culture language. If the first language does not match the client’s culture set, then the chosen language will be the Shell UI language.   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. Back in CMD, type **setup.exe /download addspanish.xml**. 7. Press Enter. Office will begin the download. 8. Back in CMD, type **setup.exe /configure addspanish.xml** and press Enter. 9. Office will begin the installation. 10. Click **Close**. 11. Type **Control Panel** inthe “Type here to search” and press Enter. 12. Click on **Programs**. 13. Click on **Programs and Features**. 14. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

## Enterprise Managed Deployment using Configuration Manager

In this activity, you will deploy Microsoft 365 Apps for enterprise using Configuration Manager and configure updating for Microsoft 365 Apps.

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Share for Microsoft 365 Apps Package and Updates | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column, record the version number of the current and previous month. 3. Logon to CM1 as (corp\labadmin). 4. On the taskbar, open File Explorer and browse to **C:\Packages** and create two folders named **OfficeConfigMan** and **OfficeConfigManUpdates**. | |
| Enable Management of Microsoft 365 Apps Client Agent | 1. In the Configuration Manager Console, browse to **Administration | Client Settings**. 2. Double-click on **Default Client Settings**. 3. Select **Software Updates**. 4. For **Enable management of the Office 365 Client Agent**, from the drop-down box select **Yes**. 5. Click **OK**. | |
| Enable and Configure Microsoft 365 Apps Software Updates | 1. Select **Administration**. 2. Expand **Site Configuration**. 3. Select **Sites**. 4. Click **Settings |** **Configure Site Components | Software Update Point**. 5. Under the **Classifications** tab, uncheck all options and only select **Updates**. 6. Under the **Products** tab, uncheck all options and only select **Office 365 Client**.   **Note:** If **Office 365 Client** is not listed, execute a full synchronization of updates and repeat above steps.   1. Under the **Languages** tab, uncheck all options and only select **English**. 2. Click **Apply | OK**. 3. Browse to **Software Library**. 4. Expand **Office 365 Client Management**. 5. Click **Office 365 Updates**. 6. Click **Synchronize Software Updates**. Click **Yes**.   **Note:** Please be patient for the sync to complete, which will take some time. | |
| Create a Folder and a Collection | 1. Browse to **Assets and Compliance | Device Collections**. Right-click **Device Collections** and click **Folder | Create Folder**. 2. Enter a name **Microsoft 365 Apps** and click **OK**. 3. Expand **Device Collections**, right-click **Microsoft 365 Apps** folder and click **Create Device Collection**. 4. Enter a name **Microsoft 365 Apps MC**. Click **Browse**. 5. Under **Device Collections**, select **Root**, select **All Systems** and click **OK**. 6. On the General page, click **Next**. 7. On the Membership Rules page, click **Next**. Click **OK** on the Configuration Manager prompt. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. 10. Browse to **Assets and Compliance | Devices**, right-click on the **CLIENT2** virtual machine, click **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 11. Under **Device Collections**, select **Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 12. Under **Device Collections | Microsoft 365 Apps**, right-click on **Microsoft 365 Apps MC** and click **Update Membership | Yes** and then refresh once to ensure that the **CLIENT2** virtual machine is a member of this collection. | |
| Create and Deploy a Microsoft 365 Apps Package | 1. Click **Software Library**. 2. Click **Office 365 Client Management** and click **Office 365 Installer**. 3. Specify the following on the Application Settings Page, and click **Next**.   Name: **Microsoft 365 Apps MC**  Content Location: **\\CM1\Packages$\OfficeConfigMan**   1. On the Office Settings page, click **Go to the Office Customization Tool**. 2. On the Deployment settings page, enter the following and click **Next**: 3. Under **Products and releases**, under **Architecture**, select **64-bit**. 4. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 5. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier for the previous month and click **Next**. 6. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 7. Under **Installation**, click **Next**. 8. Under **Update and upgrade**, ensure that **Uninstall any MSI versions of Office, including Visio and Project** is turned ON and then click **Next**. 9. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 10. Under **General**, click **Next**. 11. Under **Application preferences**, click **Finish**. 12. Click **Review**, select **Keep Current Settings**, click **OK**, review the details and click **Submit**. 13. On the Deployment page, select **Yes** and click **Next**. 14. On the General page, click **Browse…** next to Collection. 15. Under **Device Collections | Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 16. Select **Automatically distribute content for dependencies** and click **Next**. 17. On the Content page, click **Add | Distribution Point**. 18. Select **CM1.CORP.CONTOSO.COM** and click **OK**. 19. Click **Next**. 20. On the Deployment Settings page, specify the following and click **Next**.   Action: **Install**  Purpose: **Required**  Other 4 Checkboxes: **Unchecked**   1. On the Scheduling page, select **As soon as possible after the available time** and click **Next**. No other checkboxes to be selected. 2. On the User Experience page, select **Display in Software Center and show all notifications**, check all the **4 checkboxes** below and click **Next**. 3. On the Alerts page, click **Next**. No checkboxes to be selected. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. This will download the content to the share specified, create the required Application, Deployment Type and Deployment as well as distribute the content to the Distribution Point. | |
| **Complete these steps on the CLIENT2 virtual machine.**  **Note: Uninstall any existing versions of Microsoft 365 Apps before performing this lab and reboot once.** | | |
| User Experience with the Download and Installation of Microsoft 365 Apps Package on the Client Side | 1. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Application Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. After a few minutes, the package will start downloading and installing after a notification. 4. The installation of the package can be validated in the **Programs and Features** once installed. 5. In the Configuration Manager Properties, **Actions** tab, select **Hardware Inventory Cycle** and click **Run Now**. Click **OK**. | |
| **Complete these steps on the CM1 virtual machine.** | | |
| Microsoft 365 Apps Readiness | You can use Configuration Manager 2002 to identify devices with high confidence that are ready to upgrade to Microsoft 365 Apps for enterprise. This integration provides insights into any potential compatibility issues with Office add-ins and macros used in your environment. Then you can use Configuration Manager to deploy Office to ready devices. The existing Microsoft 365 client management dashboard includes a tile called **Office 365 ProPlus Upgrade Readiness**. There are few prerequisites that need to be in place.   1. Hardware inventory must be enabled in the client settings. To verify, in the Configuration Manager Console, browse to **Administration | Client Settings**. Double-click on **Default Client Settings** and click **Hardware Inventory**. Ensure that **Enable hardware inventory on clients** is set to **Yes**. Now click **Set Classes** next to **Hardware inventory classes** and ensure **Office 365 ProPlus Configurations**, **Office add-ins**, **Office document metrics** and **Office VBA scan summary** are selected. 2. The device needs connectivity to the Office content delivery network (CDN) to download an add-in readiness file. If the device can’t download this file, the add-ins state is *Needs review*.   For more information, refer to [https://docs.microsoft.com/en-us/configmgr/sum/deploy-use/office-365-dashboard#bkmk\_o365\_readiness](https://docs.microsoft.com/en-us/sccm/sum/deploy-use/office-365-dashboard#bkmk_o365_readiness)   1. To access the **Office 365 ProPlus Upgrade Readiness** tile, in the Configuration Manager Console, browse to **Software Library | Office 365 Client Management**. | |
| **Complete these steps on the CM1 virtual machine.** | | |
| Create and Deploy a Microsoft 365 Apps Software Update | 1. Once the sync is complete, browse to **Software Library |** **Office 365 Client Management | Office 365 Updates**. **Search** for **Current Month Version of Current Channel** with the **x64 architecture**, select and right-click **the update** and click **Create Software Update Group**. 2. Enter a name **Microsoft 365 Apps MC Updates** and click **Create**. 3. Browse to **Software Library | Software Updates | Software Update Groups**. Select **Microsoft 365 Apps MC Updates** and click **Deploy** from the ribbon bar. 4. For the Collection, click **Browse…** 5. Under **Device Collections | Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 6. On the General page, click **Next**. 7. On the Deployment Settings page, specify the following and click **Next**.   Type of deployment: **Required**  Detail level: **Only success and error messages**  No other checkbox to be selected   1. On the Scheduling page, specify the following and click **Next**.   Time based on: **Client local time**  Software available time: **As soon as possible**  Installation deadline: **As soon as possible**  No other checkbox to be selected   1. On the User Experience page, specify the following and click **Next**.   User notifications: **Display in Software Center and show all notifications**  Under **Deadline behaviour**, check the box next to **Software updates installation**  No other checkbox to be selected   1. On the Alerts page, click **Next**. No checkboxes to be selected. 2. On the Deployment Package page, select **Create a new deployment package** and specify the following and click **Next**.   Name: **Microsoft 365 Apps MC Updates**  Package source: **\\CM1\Packages$\OfficeConfigManUpdates**   1. On the Distribution Points page, click **Add | Distribution Point**. 2. Select **CM1.CORP.CONTOSO.COM** and click **OK**. 3. On the Distribution Points page, click **Next**. 4. On the Download Location page, select **Download software updates from the Internet** and click **Next**. 5. On the Language Selection page, select **English (United States)** for **Office 365 Client Update** and click **Next**. 6. On the Download Settings page, specify the following and click **Next**.   Deployment options: **Download software updates from distribution point and install** as well as **Download and install software updates from the distribution points in site default boundary group**   1. On the Summary page, click **Next**. 2. On the Completion page, click **Close**. This will download the content to the share specified, create the required Deployment Package and Deployment as well as distribute the content to the Distribution Point. | |
| **Complete these steps on the CLIENT2 virtual machine.** | | |
| User Experience with the Download and Installation of Microsoft 365 Apps Software Update on the Client Side | 1. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**. 4. The software update will start downloading and installing.   **Note:** It can take some time for the machine to be detected in Configuration Manager for the **“Required”** update. Run **Hardware Inventory Cycle**, **Software Inventory Cycle** and **Software Updates Scan Cycle** on the clients to fasten the process.   1. The installation of the package can be validated in the **Programs and Features**. | |
| **Microsoft Teams MSI Installation using Configuration Manager**  **For more information, refer to -** <https://docs.microsoft.com/en-us/microsoftteams/msi-deployment> | | |
| **Complete these steps on the CLIENT2 virtual machine.** | | |
| Uninstall Microsoft 365 Apps from the Previous Labs | 1. **Uninstall** any existing versions of **Microsoft 365 Apps** from **Programs and Features**. 2. For **Microsoft Teams** specifically (if exists):  * Delete the directory recursively under **%localappdata%\Microsoft\Teams\*\**. * Delete the **HKEY\_CURRENT\_USER\Software\Microsoft\Office\Teams\PreventInstallationFromMsi** registry value. | |
| **Complete these steps on the CM1 virtual machine.** | | |
| Create a Folder and Download the Microsoft Teams MSI | 1. Browse to **C:\Packages**. 2. Create a **Folder** by the name **MSTeamsMSI**. 3. In the **MSTeamsMSI** Folder, **download** the **Microsoft Teams MSI** from <https://teams.microsoft.com/downloads/desktopurl?env=production&plat=windows&arch=x64&managedInstaller=true&download=true> | |
| Create a Device Collection and Add the Machine to that Collection | 1. In the Configuration Manager Console, browse to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. In the **General** page, enter the following and click **Next**:   Name: **Microsoft Teams MSI**  Click **Browse...**Select **All Systems**. Click **OK**   1. In the **Membership** Rules page, enter the following and click **Next**:   Click **Add Rule > Direct Rule**  Click **Next**  Enter **CLIENT2** and click **Next**  Select **CLIENT2** and click **Next**  Click **Next** and then click **Close**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Ensure that **CLIENT2** is in the **Microsoft Teams MSI** collection. | |
| Create and Deploy the Microsoft Teams MSI Application | 1. Navigate to **Software Library > Application Management > Applications**. 2. Right-click **Applications** and click **Create Application**. 3. In the **General** page, enter the following and click **Next**:   Location: **\\CM1\Packages$\MSTeamsMSI\Teams\_windows\_x64.msi**   1. In the **Import Information** page, click **Next**. 2. In the **General Information** page, enter the following and click **Next**:   Installation program: **msiexec /i Teams\_windows\_x64.msi OPTIONS="noAutoStart=true" ALLUSERS=1**  Install behavior: **Install for system**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Now, right-click **Teams Machine-Wide Installer** and click **Deploy**. 4. In the **General** page, click **Browse...**under **Device Collections**, select **Microsoft Teams MSI** and click **OK**. 5. Click **Next**. 6. In the **Content** page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 7. In the **Deployment Settings** page, select the **Purpose** as **Required** and click **Next**. 8. In the **Scheduling** page, click **Next**. 9. In the **User Experience** page, click **Next**. 10. In the **Alerts** page, click **Next**. 11. In the **Summary** page, click **Next**. 12. In the **Completion** page, click **Close**. | |
| **Complete these steps on the CLIENT2 virtual machine.** | | |
| Retrieve Policies and Install Teams | 1. Launch the **Configuration Manager Client** applet from **Control Panel > System and Security**. 2. Go to the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 3. As soon as the notification appears click it to launch the **Software Center**. Observe the download and installation. 4. **IMPORTANT: Once the installation has been completed successfully, restart CLIENT2 once and re-login with CORP\LabAdmin.** 5. In a few moments, observe the **Microsoft Teams** icon on the desktop and the same will appear in the **Programs and Features**. | |

## Enterprise Managed Deployment using Microsoft Intune

In this activity, you will deploy Microsoft 365 Apps for enterprise using Microsoft Intune.

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Add Microsoft 365 Apps | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 6. In the Create app pane, under App type, select **Microsoft 365 Apps | Windows 10** and click **Select**. | |
| Configure and Deploy Microsoft 365 Apps | 1. Under **App suite information**, keep the default settings and click **Next**. 2. Under **Configure app suite**, enter/select the following and click **Next**: Leave the rest as default settings: 3. **Select Office apps**: Only select **Excel, OneDrive Desktop, OneNote 2016, Outlook, PowerPoint, Skype for Business,** and **Word** 4. **Update channel**: **Monthly** 5. **Accept the Microsoft Software License Terms on behalf of users**: **Yes** 6. **Languages**: **English** 7. Under **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 8. Under **Review + create**, review the page and click **Create**.   **Note:** This group should have already been created as part of **Section 3.2.1**. | |
| **Complete these steps on the CLIENT3 virtual machine.** | | |
| User Experience with the Download and Installation of Microsoft 365 Apps Package on the Client Side | **Note:** Ensure that the **CLIENT3** virtual machine is Azure AD Joined, enrolled into MDM, logged in as a cloud user, example TU1 and **Microsoft 365 Apps** is uninstalled if it is already installed.   1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. The Microsoft 365 Apps will download and install automatically in the background, which can be seen from the **Task Manager**, **Details** tab. 5. The installation of the package can be validated in the **Programs and Features**. | |

## LOB Deployment and Management with Microsoft Intune

### Add Windows line-of-business (LOB) apps to Microsoft Intune

Intune supports Windows line-of-business apps (.msi files only).

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Add Line-of-Business App | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 6. In the **Create app** pane, under **App type**, select **Line-of-business app** and click **Select**. |
| Configure Line-of-Business App | 1. Under **App information**, click **Select app package file**. 2. On the **App package file** blade, choose the browse button, and select a Windows installation file with the extension **.msi, .appx, or .appxbundle**. A sample msi file can be downloaded from: <https://www.7-zip.org/download.html> 3. Click **OK.** 4. Under **App information**, enter the following information and click **Next**:    1. **Name** - Enter the name of the app as it is displayed in the company portal. Make sure all app names that you use are unique. If the same app name exists twice, only one of the apps is displayed to users in the company portal.    2. **Description** - Enter a description for the app. The description is displayed to users in the company portal.    3. **Publisher** - Enter the name of the publisher of the app.    4. **App install context** – This specifies the install context to be associated with this app. For dual mode apps, select the desired context for this app. For all other apps, this is pre-selected based on the package and cannot be modified.    5. **Ignore app version** – Set this to “Yes” only for apps that are automatically updated by the app developer (such as Google Chrome).    6. **Command**-**line** **arguments** - Optionally, enter any command-line arguments that you want to apply to the .msi file when it runs, like /q.    7. **Category** - Select one or more of the built-in app categories, or a category you created. Categorizing apps makes it easier for users to find the app when they browse the company portal.    8. **Show this as a featured app in the Company Portal** - Display the app prominently on the main page of the company portal when users browse for apps.    9. **Information URL** - Optionally, enter the URL of a website that contains information about the app. The URL is displayed to users in the company portal.    10. **Privacy URL** - Optionally, enter the URL of a website that contains privacy information for the app. The URL is displayed to users in the company portal.    11. **Developer** - Optionally, enter the name of the app developer.    12. **Owner** - Optionally, enter a name for the owner of this app, for example, HR department.    13. **Notes** - Enter any notes you would like to associate with this app.    14. **Logo** - Upload an icon that is associated with the app. The icon is displayed with the app when users browse the company portal. |

### Assign Apps to Groups and Deploy with Microsoft Intune

In the following section, you will assign the Line-of-business app to users and devices.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Assign and Configure App Assignment | 1. Under **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 2. Under **Review + create**, review the page and click **Create**.   **Note:** This group should have already been created as part of **Section 3.2.1**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| User Experience with the Download and Installation of the App on the Client Side | 1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. The app will download and install automatically in the background. 5. The installation of the app can be validated in the **Programs and Features**. |

## Deploy Microsoft Teams

Now Microsoft Teams can be deployed using Configuration Manager as well as Intune using the MSI Installer.

For more information, refer to - <https://docs.microsoft.com/en-us/microsoftteams/msi-deployment>

### Install Microsoft Teams using Configuration Manager

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Uninstall Microsoft 365 Apps from the Previous Labs | 1. **Uninstall** any existing versions of **Microsoft 365 Apps** from **Programs and Features**. 2. For **Microsoft Teams** specifically (if exists):  * Delete the directory recursively under **%localappdata%\Microsoft\Teams\*\**. * Delete the **HKEY\_CURRENT\_USER\Software\Microsoft\Office\Teams\PreventInstallationFromMsi** registry value. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Folder and Download the Microsoft Teams MSI | 1. Browse to **C:\Packages**. 2. Create a **Folder** by the name **MSTeamsMSI**. 3. In the **MSTeamsMSI** Folder, **download** the **Microsoft Teams MSI** from <https://teams.microsoft.com/downloads/desktopurl?env=production&plat=windows&arch=x64&managedInstaller=true&download=true> |
| Create a Device Collection and Add the Machine to that Collection | 1. In the Configuration Manager Console, browse to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. In the **General** page, enter the following and click **Next**:   Name: **Microsoft Teams MSI**  Click **Browse...**Select **All Systems**. Click **OK**   1. In the **Membership** Rules page, enter the following and click **Next**:   Click **Add Rule > Direct Rule**  Click **Next**  Enter **CLIENT2** and click **Next**  Select **CLIENT2** and click **Next**  Click **Next** and then click **Close**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Ensure that **CLIENT2** is in the **Microsoft Teams MSI** collection. |
| Create and Deploy the Microsoft Teams MSI Application | 1. Navigate to **Software Library > Application Management > Applications**. 2. Right-click **Applications** and click **Create Application**. 3. In the **General** page, enter the following and click **Next**:   Location: **\\CM1\Packages$\MSTeamsMSI\Teams\_windows\_x64.msi**   1. In the **Import Information** page, click **Next**. 2. In the **General Information** page, enter the following and click **Next**:   Installation program: **msiexec /i Teams\_windows\_x64.msi OPTIONS="noAutoStart=true" ALLUSERS=1**  Install behavior: **Install for system**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Now, right-click **Teams Machine-Wide Installer** and click **Deploy**. 4. In the **General** page, click **Browse...**under **Device Collections**, select **Microsoft Teams MSI** and click **OK**. 5. Click **Next**. 6. In the **Content** page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 7. In the **Deployment Settings** page, select the **Purpose** as **Required** and click **Next**. 8. In the **Scheduling** page, click **Next**. 9. In the **User Experience** page, click **Next**. 10. In the **Alerts** page, click **Next**. 11. In the **Summary** page, click **Next**. 12. In the **Completion** page, click **Close**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Retrieve Policies and Install Teams | 1. Launch the **Configuration Manager Client** applet from **Control Panel > System and Security**. 2. Go to the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 3. As soon as the notification appears click it to launch the **Software Center**. Observe the download and installation. 4. **IMPORTANT: Once the installation has been completed successfully, restart CLIENT2 once and re-login with CORP\LabAdmin.** 5. In a few moments, observe the **Microsoft Teams** icon on the desktop and the same will appear in the **Programs and Features**. |

### Install Microsoft Teams using Intune

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Uninstall Microsoft 365 Apps from the Previous Labs | 1. **Uninstall** any existing versions of **Microsoft 365 Apps** from **Programs and Features**. 2. For **Microsoft Teams** specifically (if exists):  * Delete the directory recursively under **%localappdata%\Microsoft\Teams\*\**. * Delete the **HKEY\_CURRENT\_USER\Software\Microsoft\Office\Teams\PreventInstallationFromMsi** registry value. |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create a Folder and Download the Microsoft Teams MSI | 1. In the **C:\** drive, create a **Folder** by the name **MSTeamsMSI**. 2. In the **MSTeamsMSI** Folder, **download** the **Microsoft Teams MSI** from <https://teams.microsoft.com/downloads/desktopurl?env=production&plat=windows&arch=x64&managedInstaller=true&download=true> |
| Add, Configure and Assign the Microsoft Teams MSI Application | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 3. On the left navigation bar, click **All services > search and click Intune > Intune**. 4. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 5. In the Create app pane, under App type, select **Other | Line-of-business app** and click **Select**. 6. Under the **App information** tab, click **Select app package file**, **browse** to **C:\MSTeamsMSI\ Teams\_windows\_x64.msi**, click **Open**, click **OK**. 7. Under the **App information** tab, enter the following details and click **Next**:  * Publisher: **Microsoft**  1. Under the **Assignments** tab, enter the following details and click **Next**:  * Under **Required**, click **+ Add group** * Type **Sales**, select it and click **Select**  1. Under the **Review + create** tab, click **Create**.   **Note:** Wait for the Teams Machine-Wide Installer to upload. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| User Experience with the Download and Installation of Microsoft Teams on the Client Side | **Note:** Ensure that the **CLIENT3** virtual machine is Azure AD Joined, enrolled into MDM, logged in as a cloud user, example TU1 and **Microsoft 365 Apps** is uninstalled if it is already installed.   1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. After a moment, a **Teams Installer** folder will be created in **C:\Program Files (x86)**. 5. **IMPORTANT: Restart CLIENT3 once and re-login with TU1 credentials.** 6. In a few moments, observe the **Microsoft Teams** icon on the desktop and the same will appear in the **Programs and Features**. Also, notice Microsoft Teams is installed in the user profile in **%localappdata%\Microsoft\Teams\*\**. Microsoft Teams will auto-launch and automatically login as **TU1**. |

## Assignment Filters

After you've [added an app to Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/apps-add), you can assign the app to users and devices. You can also create filters to narrow the assignment scope of a policy. For example, use filters to target devices with a specific OS version or a specific manufacturer, or target only personal devices or only organization-owned devices. For more details on using filters when assigning apps in EndPoint Manager, see: [Create filters in Microsoft Intune - Azure | Microsoft Docs](https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters).

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps on a browser** | |
| Create device filters | 1. Sign in to the [Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Tenant administration** > **Filters (preview)** > **Try out the filters (preview) feature**. 3. Set **Filters (preview)** to **On**. 4. Select **Tenant administration** > **Filters (preview)** > **Create**. 5. In **Basics**, enter the following properties:    * + **Filter name**: Enter a descriptive name for the filter. Name your filters so you can easily identify them later. For example, a good filter name is **Windows OS version filter**.      + **Description**: Enter a description for the filter. This setting is optional but recommended.      + **Platform**: Select your platform. 6. Select **Next**. 7. In **Rules**, create a rule using the **rule builder.** (You can also use the rule syntax.) **Rule builder**:    * **And/Or**: After you add an expression, you can add to the expression using the and/or options.    * **Property**: Select a property for your rule, such as device or operating system SKU.    * **Operator**: Select the operator from the list, such as equals or contains.    * **Value**: Enter the value in your expression. For example, enter 10.0.18362 for the OS version, or Microsoft for the manufacturer. 8. **Add expression**: After you add the property, operator, and value, select **Add expression.** The expression you created is automatically added to the rule syntax editor. 9. Select **Next**. 10. In **Scope tags** (optional), assign a tag to filter the profile to specific IT groups, such as US-NC IT Team or JohnGlenn\_ITDepartment. For more information about scope tags, see [Use RBAC and scope tags for distributed IT](https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags). Select **Next**. 11. In **Review + create**, review your settings. When you select Create, your changes are saved. The filter is created, and ready to be used. The filter is also shown in the filters list. |
| Assign apps to groups and apply filters. | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Apps** > **All apps**. 3. In the **Apps** pane, select the app you want to assign. (e.g. XML Notepad). Select **Properties.** 4. Click edit **next** to **Assignments**. 5. Select **Add group** to add a group of users that you want assigned to the app. Click **Select**. 6. Under **Required**, click a group under Select Groups at right. Click **Select**. 7. Under **Required**, under the Filter column, click **none**. 8. Under Filters, select the **Exclude filtered devices in assignment**. Select the devices in the group that you want excluded from the app. Click **Select**. 9. To save your changes, select **Review + save** > **Save**. When the device checks in with the Intune service, the properties defined in the filter are evaluated, and determine if the app or policy should be applied. |

# Appendix A: Windows Virtual Desktop

Windows Virtual Desktop is a desktop and app virtualization service that runs on the cloud.

Here’s what you can do when you run Windows Virtual Desktop on Azure:

* Set up a multi-session Windows 10 deployment that delivers a full Windows 10 with scalability.
* Virtualize Microsoft 365 Apps and optimize it to run in multi-use virtual scenarios.
* Provide Windows 7 virtual desktops and free Extended Security Updates.
* Bring your existing Remote Desktop Services (RDS) and Windows Server desktops and apps to any computer.
* Virtualize both desktops and apps.
* Manage Windows 10, Windows Server, and Windows 7 desktops and apps with a unified management experience.

For more information, refer to <https://docs.microsoft.com/en-in/azure/virtual-desktop/overview> and every sub-section of this article.

## Windows Virtual Desktop – Prepare

This section of the lab explains how to prepare for Windows Virtual Desktop – a cloud-based virtualization solution running on Microsoft Azure. Windows Virtual Desktop is an elastically scalable service to deliver remote desktop and remote app experiences – without having to manage the underlying server infrastructure. As part of this lab, we will setup the prerequisites and tools provided by Microsoft to get ready to provision your first Windows Virtual Desktop host pool.

### Prerequisites

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Set up an Active Azure Subscription with Global Admin Permissions | 1. Follow **Section 3.2.1 – Setup Azure and Microsoft 365 – Steps 1-24**. |
| Set up Microsoft 365 E3 Trial | 1. Follow **Section 3.2.1 – Setup Azure and Microsoft 365 – Steps 25-29**. |
| Set up Azure Test Users | 1. Follow **Section 3.2.1 – Setup Azure and Microsoft 365 – Steps 30-47**. |
| Assign Microsoft 365 E3 Licenses | 1. Follow **Section 3.2.3 – Enable and Configure Cloud Services – Steps 1-8**.   **Note:** Ignore EM+S Licenses as part of this sub-section. |

### Set up and Configure Azure AD Domain Services

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Configure Azure AD Domain Services | 1. Navigate in private mode to <https://portal.azure.com> 2. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 3. In the Azure Portal, from the top left-hand corner, click **Create a resource**. 4. In the search box enter, **Azure AD Domain Services** and select **Azure AD Domain Services**. 5. On the Azure AD Domain Services page, click **Create**. 6. Under the **Basics** tab, enter the following information and then click **Next**:  * **Subscription**: Select your appropriate subscription from the drop-down menu * **Resource group**: Click **Create new**, enter **ADDSRG** and click **OK** * **DNS domain name**: Ensure **<AzureDomainName>.onmicrosoft.com** is present * **Location**: Select the appropriate location from the drop-down menu, example: **(US) East US** * Keep the default option for **SKU** * **Forest type**: Select **User** as the default option  1. Under the **Networking** tab, enter the following information and then click **Next**:  * **Virtual network**: Keep the default as **(new) aadds-vnet** * **Subnet**: Keep the default as **(new) aadds-subnet (10.0.0.0/24)**  1. Under the **Administration** tab, enter the following information and then click **Next**:  * **AAD DC Administrators**: Click **Manage group membership**. Click **+ Add members**. In the search box enter, **LabAdmin**, select **LabAdmin@<AzureDomainName>.onmicrosoft.com** and then click **Select**   **Note:** To go back to the previous page, click **Create Azure AD Domain Services** at the top of the page or scroll to the left.   * **Notifications**: Ensure **All Global Administrators of the Azure AD directory** and **Members of the AAD DC Administrations group** are selected  1. Under the **Synchronization** tab, enter the following information and then click **Next**:  * **Synchronization type**: Select **All** as the default option  1. Under the **Review + create** tab, after the validation has passed, review the settings and click **Create**. 2. On the **You should know...** message, click **OK**.   **Note:** It will take about half an hour or so for Azure AD Domain Services to be created, so please be patient.   1. Once the deployment is completed, click **Go to resource**.   **Note:** You will notice the message "The managed domain is being provisioned. This operation will take a while." So please wait until this message disappears for another around half an hour.   1. Once the state of the Azure AD Domain Services is "**Running**", click **Configure** to update DNS server settings for your virtual network. 2. Close all browser windows. |
| Enable Azure AD Domain Services Password Hash Synchronization for Cloud-Only User Accounts | 1. Go to the **Azure AD Access Panel** page in private mode at <https://myapps.microsoft.com> and sign in with **TU1@<AzureDomainName>.onmicrosoft.com**. 2. In the top-right corner, select **Test User1 or TU1**, then click **Profile** from the drop-down menu. 3. On the Profile page, click **Change password**. 4. On the change password page, enter the existing (old) password, then enter and confirm a new strong password. 5. Click **Submit** and sign out. 6. Repeat **Steps 15-19** for the user accounts - **Test User2 or TU2** and **LabAdmin**.   **Note:** It takes a few minutes after you've changed your password for the new password to be usable in Azure AD Domain Services and to successfully sign in to computers joined to the managed domain. Before creating the host pool, wait for atleast half an hour for synchronization to take place. |

## Windows Virtual Desktop – Deploy

This section of the lab explains how to deploy Windows Virtual Desktop, including the wizard-based process to provision a Windows Virtual Desktop host pool and how to customize remote desktops and RemoteApps for your users.

### Create a Host Pool by using the Azure Portal

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Enable the Resource Provider | 1. Sign in to the Azure Portal as **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search and click Subscriptions**. 3. Click the appropriate **Subscription**, scroll down and click **Resource providers**. 4. Search and select **Microsoft.DesktopVirtualization** and click **Register**. 5. Click **Refresh** and wait until the status changes to **Registered**. |
| Begin the Host Pool Setup Process | 1. Enter **Windows Virtual Desktop** into the search bar, then find and select **Windows Virtual Desktop** under **Services**. 2. In the Windows Virtual Desktop overview page, select **Create a host pool**. 3. Under the **Basics** tab, enter the following and click **Next: Virtual Machines**:  * **Subscription**: Select your appropriate subscription from the drop-down menu * **Resource group**: Click **Create new**, enter **WVDRG** and click **OK** * **Host pool name**: Enter a name for the host pool that’s unique within the Windows Virtual Desktop tenant, example: **WVDPoC01** * **Location**: Select the appropriate location from the drop-down menu, example: **East US** * **Host pool type**: Select **Pooled**. With this option selected, users are directed to the best available session host in the pool to utilize multi-session virtual machines. With the **Personal** option selected, each user will have their own virtual machine * **Max session limit**: Enter **2** * **Load balancing algorithm**: Select **Breadth-first**  1. Under the **Virtual Machines** tab, enter the following information and then click **Next : Workspace**:  * **Add virtual machines**: Select **Yes** * **Resource group**: Leave it to **Defaulted to same as host pool** * **Virtual machine location**: Select the appropriate location from the drop-down menu, example: **East US** * **Virtual machine size**: Select your appropriate size or go with the default size, example: **B2ms** * **Number of VMs**: Enter **2** * **Name prefix**: Enter a prefix for the names of the virtual machines. For example, if you enter the name "**prefix**," the virtual machines will be called "prefix-0," "prefix-1," and so on * **Image type**: Select **Gallery** * **Image**: Select **Windows 10 Enterprise multi-session, Version 20H2 + Office 365 ProPlus** * **OS disk type**: Select a suitable disk type from the drop-down menu, example: **Standard HDD** * **Virtual network**: Select the same virtual network associated with your Azure AD Domain Services: **aadds-vnet** * **Subnet**: Select the same subnet associated with your Azure AD Domain Services: **aadds-subnet (10.0.0.0/24)** * **Public IP**: Select **Yes** * **Configure SKU**: Select **Basic** * **Configure assignment**: Select **Dynamic** * **Network security group**: Select **Basic** * **Public inbound ports**: Select **Yes** * **Inbound ports to allow**: Select **HTTP**, **HTTPS** and **RDP** * **Specify domain or unit**: Select **Yes** * **Domain to join**: Enter the domain name of the Azure AD Domain Services. example: **<AzureDomainName>.onmicrosoft.com** * **Organizational Unit path**: Keep the default as **blank** * **AD domain join UPN**: Enter **LabAdmin@<AzureDomainName>.onmicrosoft.com** * **Password**: Enter the password for **LabAdmin@<AzureDomainName>.onmicrosoft.com** * **Confirm password**: Confirm the password for **LabAdmin@<AzureDomainName>.onmicrosoft.com**  1. Under the **Workspace** tab, enter the following information and then click **Next : Tags**:  * **Register desktop app group**: Select **Yes** * **To this workspace**: Select **Create new**, enter **WVDPoCWorkspace01** and then click **OK**  1. Under the **Tags** tab, click **Next: Review + create**. 2. Under the **Review + create** tab, after the validation has passed, review the settings and click **Create**.   **Note:** Depending on how many VMs you’re creating, this process can take 30 minutes or more to complete.   1. Once the deployment has completed, enter **Windows Virtual Desktop** into the search bar, then find and select **Windows Virtual Desktop** under **Services**. 2. Click **Application groups** and select **WVDPoC01-DAG** which is the default desktop app group created. 3. Under **Manage**, click **Assignments**. 4. Click **+ Add**, type **TU**, select **TU1** and **TU2**, click **Select** and ensure that both the users show up in the **WVDPoC01-DAG | Assignments**. |

### Connect to Windows Virtual Desktop Resources

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Connect with the Web Client | **Note:** Sign in with a user account one at a time.   1. Open Internet Explorer in private mode and go to <https://rdweb.wvd.microsoft.com/arm/webclient>. 2. Sign in with **TU1@<AzureDomainName>.onmicrosoft.com** OR **TU2@<AzureDomainName>.onmicrosoft.com**. 3. You should be able to see a desktop icon. Once you click on that, it will ask you to select the relevant options in order to access local resources, like Clipboard and Printer. Click **Allow**. 4. It will then ask you to enter the credentials again. Enter the Username: **TU1@<AzureDomainName>.onmicrosoft.com** OR **TU2@<AzureDomainName>.onmicrosoft.com** and the **Password** and then click **Submit**. 5. You will then be logged in to the Windows Virtual Desktop as **TU1** OR **TU2** and will be assigned a VM out of the pool. It will have Microsoft 365 Apps installed and you can maximize/minimize the screen. 6. Sign out of the Windows Virtual Desktop, sign out from the browser and close the browser. |

### Manage App Groups

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create a Remote App Group | 1. Sign in to the Azure Portal as **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 2. Enter **Windows Virtual Desktop** into the search bar, then find and select **Windows Virtual Desktop** under **Services**. 3. Click **Application groups** and then click **+ Add**. 4. Under the **Basics**, enter the following information and then click **Next: Assignments**:  * **Subscription**: Select your appropriate subscription from the drop-down menu * **Resource group**: Select **WVDRG** from the drop-down menu * **Host pool**: Select **WVDPoC01** from the drop-down menu * **Location**: Just view the location: **East US** * **Application group type**: Select **RemoteApp** * **Application group name**: Enter **WVDPoCRemoteAppGroup01**  1. Under the **Assignments** tab, enter the following information and then click **Next: Applications**:  * Click **+ Add Azure AD users or user groups** * Type **TU**, select **TU1** and **TU2**, click **Select** and ensure that both the users show up  1. Under the **Applications** tab, enter the following information and then click **Next: Workspace**:  * Click **+ Add applications** * **Application source**: Select **Start menu** * **Application**: Select **Word** * **Display name**: Enter **Word** * **Description**: Enter **Word RemoteApp** * **Application path**, **Icon path** and **Icon index** will be **greyed out** * **Require command line**: Select **No** * Click **Save**  1. Under the **Workspace** tab, enter the following information and then click **Next : Tags**:  * **Register application app group**: Select **Yes** * The **WVDPoCWorkspace01** will be automatically selected and greyed out  1. Under the **Tags** tab, click **Next: Review + create**. 2. Under the **Review + create** tab, after the validation has passed, review the settings and click **Create**. |

### Connect to Windows Virtual Desktop Resources

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Connect with the Web Client | **Note:** Sign in with a user account one at a time.   1. Open Internet Explorer in private mode and go to <https://rdweb.wvd.microsoft.com/arm/webclient>. 2. Sign in with **TU1@<AzureDomainName>.onmicrosoft.com** OR **TU2@<AzureDomainName>.onmicrosoft.com**. 3. You should be able to see an icon of Microsoft Word. Once you click on that, it will ask you to select the relevant options in order to access local resources, like Clipboard and Printer. Click **Allow**. 4. It will then ask you to enter the credentials again. Enter the Username: **TU1@<AzureDomainName>.onmicrosoft.com** OR **TU2@<AzureDomainName>.onmicrosoft.com** and the **Password** and then click **Submit**. 5. Microsoft Word will then launch and signed in as **TU1** OR **TU2** and the look and feel of the application will be as if it is installed locally and you can maximize/minimize the application window. 6. Close Microsoft Word, sign out from the browser and close the browser. |

## Windows Virtual Desktop – Optimize

This section of the lab explains how to optimize Windows Virtual Desktop, including how to customize a basic environment to take advantage of new storage, file management, and automated scaling options.

### Separate User Profiles from Virtual Machines with FSLogix Profiles

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **This section is just an overview for informational purposes and explains the concepts.**  **For more information, refer to** <https://docs.microsoft.com/en-us/learn/modules/m365-optimize-wvd/provision-fslogix> | |
| Separate User Profiles from Virtual Machines with FSLogix Profiles | You can use FSLogix profiles to separate user profiles from virtual machines, persist these profiles as user-assigned virtual disks in Azure storage, Azure NetApp Files, and Storage Spaces Direct, and then dynamically attach them to a user. Each time the user signs in to a remote resource, their profile is attached to the resource, and they're able to access all of their data.  Compared to classic roaming user profiles in Windows, separating the user profiles and data enables a seamless roaming experience for apps that rely on %localappdata% locations, like Outlook and OneDrive. It's fast and stateful - as far as users can tell, their data loads as fast as locally stored data. FSLogix profiles let you use cached mailboxes for local-like access to email and OneDrive Files on Demand. |

### Configure OneDrive in Microsoft 365 in Windows Virtual Desktop Host Pools

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **This section is just an overview for informational purposes and explains the concepts.**  **For more information, refer to** <https://docs.microsoft.com/en-us/learn/modules/m365-optimize-wvd/configure-onedrive> | |
| Configure OneDrive in Microsoft 365 in Windows Virtual Desktop Host Pools | In Windows Virtual Desktop, you can leverage Office and OneDrive Group Policy settings to direct files to Microsoft 365 storage locations. This lets you take advantage of the 1 TB and greater storage available in OneDrive, plus collaboration capabilities like improved sharing, seamless secure access across devices, improved discovery of recently used files, and real-time co-authoring with co-workers and partners.  You can use Active Directory Group Policy with Microsoft 365 Apps and Office 2019 Volume Licensing editions. You can download administrative template files (.ADMX) from the <https://www.microsoft.com/download/details.aspx?id=49030>.  After you provision accounts for OneDrive, you can use policies to configure Office default save locations and implement OneDrive Known Folder Move. |
| Office Group Policy Settings | Configure Office default file locations in the Group Policy Editor (gpedit.msc), typically in **User Configuration\Administrative Templates (Your Office App)\App Options\File Locations**. (The exact location for this setting varies slightly per app.) These settings are frequently used for Excel, Word, and PowerPoint in Remote Desktop Services environments. |
| OneDrive Group Policy Settings | For the OneDrive policy settings, first import administrative templates for OneDrive from **%localappdata%\Microsoft\OneDrive\BuildNumber\adm** on an updated Windows 10 device. In the Group Policy Editor, set the following OneDrive settings in **Computer Configuration\Administrative Templates\OneDrive**:   * **Silently sign in to users to OneDrive sync with their Windows credentials** – These need to match synched accounts in Azure AD. * **Silently move known folders to OneDrive** – This setting ensures documents, pictures, and desktop folders are synched to OneDrive accounts. * **Use OneDrive Files on Demand** – This setting turns on the capability and prevents users from turning it off. * **Set maximum size of a user’s OneDrive that can download automatically** – This setting prevents using too much local storage in virtual machines.   Because OneDrive services are part of Microsoft’s cloud infrastructure, users can easily access files stored in OneDrive. The proximity and connection speeds between VMs in Windows Virtual Desktop and OneDrive services mean that even large files can be hydrated quickly. |

### Migrate Files from Local File Shares into Azure Storage using Azure File Sync

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **This section is just an overview for informational purposes and explains the concepts.**  **For more information, refer to** <https://docs.microsoft.com/en-us/learn/modules/m365-optimize-wvd/migrate-files> | |
| Migrate Files from Local File Shares into Azure Storage using Azure File Sync | If your current Remote Desktop architecture uses file shares in Windows Server to access shared files, folders, and locations, you can use Azure File Sync to synchronize your on-premises file server contents into the same file share location you created for user profile virtual disks. You can also use Azure NetApp files with local NetApp technology to migrate files and properties to Azure storage.  Azure File Sync enables seamless access for files that were initially generated in Azure or on-premises - Windows Virtual Desktop session hosts can access the files from a nearby location stored in Azure. You can also map drives using SMB 3.0 protocols (as you may have already configured if you’re migrating from on-premises Remote Desktop Services infrastructure to Windows Virtual Desktop), so users don’t experience changes in their workflow.  If you’re already using FSLogix in your on-premises implementation of Remote Desktop Services, you can also use Azure File Sync to migrate and synchronize your user profile virtual disks into Azure storage to use with Windows Virtual Desktop. |

### Automate Depth and Breadth Scaling for Windows Virtual Desktop Host Pools

|  |  |
| --- | --- |
| Task | Detailed Steps |
| **This section is just an overview for informational purposes and explains the concepts.**  **For more information, refer to** <https://docs.microsoft.com/en-us/learn/modules/m365-optimize-wvd/configure-automation> | |
| Automate Depth and Breadth Scaling for Windows Virtual Desktop | Windows Virtual Desktop provides tools and approaches to automate scaling VM resources in your host pools. One of the primary benefits to hosting Remote Desktop Service in the cloud is that you can shut down compute resources to save costs during off-peak hours, and then restart them either on a schedule or dynamically, based on session host utilization.  The Windows Virtual Desktop scaling scripts include logic to periodically determine activity levels in VMs before draining underutilized user session hosts and shutting them down. During off-peak usage (usually after hours) the script can reduce the number of running VMs; during peak usage, the script can dynamically provision additional VMs when user density exceeds defined thresholds that trigger scaling.  Download the scaling scripts from the scaling script repository - <https://aka.ms/WVDscaling> in GitHub. They currently run in the context of a connected VM using scheduled tasks. In the future, scaling operations will use Azure Automation. |

# Appendix B - Compatibility

## Convert a Win32 app to a UWP app

The Windows 10 Desktop Bridge provides consumer and enterprise developers a low friction path to migrate their Win32 apps to Windows 10 Universal Windows Platform (UWP). In doing so, developers can take advantage of Windows 10 features and app distribution not available to traditional Win32 apps. Win32 apps using the Desktop Bridge also provide a safer and cleaner virtualized runtime environment. For more information on the Desktop Bridge see: <https://developer.microsoft.com/en-us/windows/bridges/desktop>

This Lab provides a walkthrough of converting a Win32 app to a UWP using the Desktop App Converter.

**Prerequisites:**

Download a **Windows 10 1903** ISO from MSDN and create a virtual machine in Hyper-V with the specifications and steps mentioned in **Section 2.3.5.5**.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on a Windows 10 1903 virtual machine. (At the moment, the Windows Desktop App Converter Base Image 18362 is available, which is the latest, for which a Windows 10 1903 virtual machine can only be used).** | |
| Install the Desktop App Converter – Version Check | 1. Make sure your computer is up-to-date with the latest Windows 10 version: Desktop App Converter. To make sure you’re on the right version, just click on the **Start** button and search and choose **Command Prompt**: at the top, you’ll see the Windows 10 build number, which should be **10.0.18362.x**. |
| Install the ‘Desktop App Converter’ | 1. The Desktop App Converter tool itself, which can be downloaded directly from the Store at the URL <https://www.microsoft.com/store/apps/9nblggh4skzw> 2. **Sign in** to the page with a Microsoft account and click ‘**Get | Install**’. Follow the onscreen instructions for the download and installation of the Desktop App Converter. |
| Download the Windows Base Image | 1. The latest base Windows image, is used as container to generate the appx package. Be aware that this file is quite big (approximately 3.5 GB). It can be downloaded from the following link: [https://www.microsoft.com/en-us/software-download/dac#](https://www.microsoft.com/en-us/software-download/dac). Click **Base Image - Build 18362** and save the file to **C:\Windows\Temp**.   **Note**: The version of the base image much match the version of the OS. In this case, we are working with **Windows 10 18362**. |
| Launch the ‘Desktop App Converter’ as Administrator | 1. Press ‘**Start**’, type ‘**Desktop App Converter**’. 2. Right-click on the **‘Desktop App Converter**’ icon and choose **Run as administrator**). Under the hood, you will notice that it’s simply a PowerShell command prompt, since it’s the technology that empowers the Desktop App Converter. |
| Install the Base Image | 1. Install the base image, by executing the following PS commands in the folder where you have copied the file you’ve previously downloaded (or, alternatively, you can pass to the **-BaseImage** parameter the full path of the file).    1. **Set-ExecutionPolicy Bypass**    2. **DesktopAppConverter.exe -Setup -BaseImage C:\Windows\Temp\Windows\_BaseImage\_DAC\_18362\_V1.wim –Verbose**   **Note:** The operation will take a while and, at some point, it may ask you to reboot the machine: the reason is that Desktop App Converter relies on a Windows 10 feature (called Containers), which isn’t installed by default. Once rebooted, the setup will continue. |
| If you get an Error | 1. If you get an error related to Containers, you can manually install the feature by right-clicking on the **Start** button, clicking **Run**, entering **appwiz.cpl**, clicking **OK** and then **Turn Windows features on or off**. You will find one called **Containers**, enable it and click **OK** and then let the installation complete and also, if asked, reboot the computer.     **Note:** The Containers feature is available only on **Windows 10 Pro or Enterprise**.   1. Now you’re all set and you’re ready to convert your first application. |
| Start the Win32 to UWP Conversion Process | **Note:** You will convert the Win32 sample app ‘Hello Centennial’. Remember that the Desktop App Converter does not modify your application binaries. It monitors the file locations and registry entries created at install time. It uses this information to create the container your Win32 app will be in.   1. **Download** the **‘Hello Centennial’** sample Win32 app’s MSI file from here: <https://github.com/qmatteoq/DesktopBridge/blob/master/1.%20Desktop%20App%20Converter/HelloCentennial.msi> 2. Create a folder called **C:\Installer** and copy the file **HelloCentennial.msi** here. 3. Create another folder called **C:\Output\HelloCentennial**. |
| Launch the ‘Desktop App Converter’ as Administrator | 1. Press ‘**Start**’, type ‘**Desktop App Converter**’. 2. Right-click on the **‘Desktop App Converter**’ icon and choose **Run as administrator**). |
| Start the Desktop App Converter Process | **Note:** DesktopAppConverter flags:   * **-Installer** is the path to the setup file we need to convert. In this case, it’s the **HelloCentennial.msi** file we’ve previously downloaded from GitHub. * **-Destination** is the folder where we want to store the output files created by the conversion process. * **-PackageName** is the name we want to give to the package. * **-Publisher** is the publisher’s name of the application. If you have some previous experience with UWP development, you’ll recall seeing this information in the manifest file of a UWP app. It’s univocally assigned by the Dev Center when you open a developer account. For the moment, for test purposes, you can just use the name you want, it’s just important that it starts with **CN=** and that it doesn’t contain spaces. * **-Version** is the version number of the app. * **-MakeAppx** means that, other than generating the folder which will contain all the files that needs to be packaged (like assets, the manifest, etc.), you want also to immediately generate the AppX package. * **-Verbose** is an optional parameter, which is useful because it will show you all the details of what’s going on during the conversion process. * **-Sign** is a parameter that allows to automatically generate the needed certificates to properly sign the AppX package. Without this digital signature, the package can’t be installed on a machine which doesn’t trust the generated certificate.  1. Download and install the Windows 10 1903 SDK: <https://go.microsoft.com/fwlink/?linkid=2083338> 2. In PowerShell type the command:   DesktopAppConverter.exe -Installer "C:\Installer\HelloCentennial.msi" -Destination "C:\Output\HelloCentennial\" -PackageName "HelloCentennial" -Publisher "CN=Awesome-Apps-Inc" -Version "1.0.0.0" -MakeAppx -Verbose -Sign   1. Inspect the **Output** folder. At the end of the process, you will get a folder structure like the following one:     The real work done by the tool can be found inside the **PackageFiles** folder:     1. As you can see, this folder looks a bit like the one that Visual Studio creates when you start a new UWP project. You have an **Assets** folder, which contains the default images to be used for the tile, the Store, or the icon in the Start menu. You have also a manifest file, the one called **AppxManifest.xml**. |
| Open the AppxManifest.xml File | 1. Notice that it’s like the manifest file of a UWP app. However, compared to a native UWP app, you’ll find a couple of differences:  * You’ll find the following **Capability**, which allows the application to run in full trust. This option is available only for converted apps, a native UWP app will not have this kind of access.   <Capabilities>  <rescap:Capability Name="runFullTrust" />  </Capabilities>   * You’ll find an **Application** entry with all the info about the Win32 process that the UWP container will launch.   <Application Id="HelloCentennial" Executable="HelloCentennial.exe" EntryPoint="Windows.FullTrustApplication"> |
| Continue Inspecting Output: Registry.Dat, VFS Folder | 1. You’ll find other files and folders that captured the MSI setup process. For example, the **Registry.dat** file contains all the changes applied to the registry. Or, if you explore the **VFS** folder, you will find all the files that are copied during the installation process. |
| Attempt to Install the Converted App (APPX) | 1. Double-click on the file **HelloCentennial.appx** and you’ll be prompted with the following dialog.     However, if you press the **Install** button out of the box, you’ll see the following error. |
| Install Certificate to Resolve Error | **Note:** The reason is that, by default, a UWP package needs to be signed with a valid certificate to be installed and this certificate needs to be trusted by the computer. When we publish a UWP app on the Store, this process is completely transparent: it’s the Store that takes care of signing the AppX package with a valid certificate during the submission process. In this case, instead, we’re trying to sideload a package without using the Store, so we need to take care of signing it.  If you remember, when we used the Desktop App Converter tool, we passed a parameter called -**Sign**, which already did the hard work for us. The package is already signed: the problem is that the certificate used for signing it, now, isn’t trusted by our computer, which leads to an installation failure.   1. To solve this problem, you’ll need to add the certificate in the **Trusted Root Certification Authority** of the computer. You’ll find it in the folder generated by the tool (the one with the AppX package) and it’s called **auto-generated.cer:** simply double-click on it, choose **Install Certificate** and, when you’re prompted where to install it, choose **Local Machine** and then the option **Place all certificates in the following store**. By pressing the **Browse** button, make sure to choose **Trusted Root Certification Authorities** and complete the process.      1. Click **Start | Settings | Update & Security | For developers** and then select **Sideload apps** and then click **Yes**. If you are unable to select the option **Sideload apps**, then launch **gpedit.msc**, browse to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > App Package Deployment** and then enable the policy **Allow all trusted apps to install** and then you will be able to select the **Sideload apps** option. |
| Retry Installing the Converted App (APPX) | 1. Double-click on the file **HelloCentennial.appx**.Uncheck **Launch when ready**. This time, after pressing the **Install** button, you will see a progress bar showing the installation status and, at the end, the window will become like the following one. |
| Find ‘HelloCentennial’ in the Start Menu | 1. Press the **Windows** key. Type **HelloCentennial**.   **Note:** Now you have a Win32 app that has been embedded into a UWP app! Notice the app will have a tile, you’ll be able to pin it to the Start menu and, if you want to uninstall it, just right-click on it, and choose Uninstall. |
| Launch the Converted App: ‘HelloCentennial’ | 1. Select the app from the Start menu to launch it. You’ll notice that it’s still a Win32 app and it will be able to create a text file on the user’s desktop just fine, without requiring any extra dialog or permission.   **Note:** You might have to download and install the prerequisites for the app to launch, which it will do automatically, which is .Net Framework 3.5 (includes 2.0 and 3.0). |

## Windows App Certification Kit

The Windows App Certification Kit can be used to test applications for the Windows Store (for Windows 10, Windows 8.1, and Windows 8), and for the Windows 10, Windows 8.1, Windows 8, and Windows 7 Windows Certification program for desktop applications.

**Note:** Revert the **Windows 10 1903** virtual machine to the latest checkpoint before starting this scenario.

**Note:** For the **Windows 10 1903** virtual machine being used, you will have to download and install Visual Studio 2019 from <https://visualstudio.microsoft.com/vs/>. The Windows App Certification Kit should be already installed as part of the SDK installation from the previous lab. Just choose the default options while installing on the **Windows 10 1903** virtual machine.

### Prepare Test Applications

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Windows 10 1903 virtual machine.** | |
| Sample Universal App | **Note**: Perform this task if the customer has no in-house built Universal App.   1. Open **File Explorer** and browse to **C:** 2. **Create** a new folder named **Temp**. 3. Open **Internet Explorer** or **Microsoft Edge** and browse to the URL below.   <https://github.com/Microsoft/Windows-appsample-coloringbook>   1. Click **Clone or download** and select **Download ZIP**. 2. **Save** the file to **C:\Temp**. 3. Once complete, browse to **C:\Temp** and **extract** the **ZIP** file in the same location. |
| Sample Desktop App | 1. Open **Internet Explorer** or **Microsoft Edge** and browse to the URL below.   <https://notepad-plus-plus.org/downloads/v7.8.2/>   1. Click **Download** and **save** the **npp.7.8.2.Installer.exe** file to **C:\Temp**. |

### Validate Universal App

This activity will perform validation of a Universal Windows Application.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Windows 10 1903 virtual machine.** | |
| Build with Visual Studio | **Note**: Perform the tasks below on the customer’s in-house built Universal App if available.   1. Click **Start** and open **Visual Studio 2019**. 2. In the **Visual Studio** window, **Sign in** with your **Microsoft Account (MSA)** if asked. 3. Click **Open a project or solution**. 4. In the **Open Project/Solution** window, browse to **C:\Temp\Windows-appsample-coloringbook-master\Windows-appsample-coloringbook-master\** 5. Select **ColoringBook.sln** then click **Open**. There might be a prompt to install some missing features. Click **Install** and follow the prompts and wait for the installation to complete. 6. In the **Security Warning for ColoringBook** window, click **OK** whenever it appears. 7. In the **Solution Explorer** pane, right-click on **ColoringBook (Universal Windows)** then select **Publish > Create App Packages**. 8. In the **Create App Packages** pane, select **Sideloading** and uncheck **Enable automatic updates** and then click **Next**. 9. In the **Select signing method** pane, select **Yes, select a certificate** and click **Create**. In the **Create a Self-Signed Test Certificate**, enter any **password** of your choice twice and click **OK**. Click **Next**. 10. In the **Select and configure packages** pane, under **Generate app bundle**, select **Never** and under **Select the packages to create and the solution configuration mappings** perform the following then click **Create**.  * Under **x86**, select **Release (x86)** * Uncheck **x64** * Uncheck **ARM**   **Note**: The build process will take around 5 minutes to complete.   1. In the **Finished creating package** pane, click **Close**. |
| Validate Post App Build | **Note**: Perform the tasks below on the customer’s in-house built Universal App if available.   1. Click **Start** and open **Windows App Cert Kit**. 2. In the **Select the validation to perform** pane, click **Validate Store App**. 3. In the **Select an app to validate** pane, click **Browse**. 4. In the **Open** window, browse to **C:\Temp\Windows-appsample-coloringbook-master\Windows-appsample-coloringbook-master\ColoringBook\AppPackages\ColoringBook\_1.x.x.x\_x86\_Test**, select **ColoringBook\_1.x.x.x\_x86.msix** then click **Open**. 5. In the **Select an app to validate** pane, click **Next**. 6. In the **Select Tests** pane, click **Next**.   **Note**: The test will take around 10 minutes to complete and the app may launch multiple times. Do not interact with the app until the validation process is complete.   1. In the **Save As** window, browse to **Desktop** and save the result as **WACK\_UniversalApp\_Result.xml**. 2. In the **View Final Report** pane, click **Click here to view the results**. 3. **Browse** and **review** the tests performed on the Universal App. 4. Once finished, close the Validation Results page. 5. In the **View Final Report** pane, click **Finish**. |

### Validate Desktop App

This activity will perform validation of a Desktop Application.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the Windows 10 1903 virtual machine.** | |
| Validate the App | **Note**: Perform the tasks below on the customer’s in-house built desktop application if available.   1. Click **Start** and open **Windows App Cert Kit**. 2. In the **Select the validation to perform** pane, click **Validate Desktop App**. 3. In the **Select the app to validate** pane, under **Setup file** browse to **C:\Temp\npp.7.8.2.Installer.exe**, under **Command line** enter **/S**, under **Application Usage Type**, select **Per Machine** then click **Next**.   **Note**: The test will take around 20 minutes to complete and the app may launch multiple times. If the app needs to install or uninstall several components or external dependencies, carefully select the option for your app.   1. In the **Save As** window, browse to **Desktop** and save the result as **WACK\_DesktopApp\_Result.xml**. 2. In the **View Final Report** pane, click **Click here to view the results**. 3. **Browse** and **review** the tests performed on the Desktop App. 4. Once finished, close the Validation Results page. 5. In the **View Final Report** pane, click **Finish**. |

# Appendix C - User File and Settings Migration

User Files and Settings Migration is necessary in PC replacement scenarios and can be accomplished by implementing services like file sync in OneDrive for Business in advance of PC replacement. Leveraging cloud file sync with OneDrive for Business and files on demand can help limit the amount of files delivered back to the new PC. In this scenario, we’ll [use Group Policy to control OneDrive sync client settings](https://docs.microsoft.com/en-us/onedrive/use-group-policy#OptInNoWizard).

## Known Folder File Migration

There are two primary advantages of moving or redirecting Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to Microsoft OneDrive for the users in your domain:

* Your users can continue using the folders they're familiar with. They don't have to change their daily work habits to save files to OneDrive.
* Saving files to OneDrive backs up your users' data in the cloud and gives them access to their files from any device.

For these reasons, we recommend moving or redirecting known folders to OneDrive if you're an enterprise or large organization. Small or medium businesses may also find this useful, but keep in mind you'll need some experience with Group Policy. For info about the end-user experience, see [Protect your files by saving them to OneDrive](https://support.office.com/article/d61a7930-a6fb-4b95-b28a-6552e77c3057).

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT7 virtual machine.** | |
| Copy .adml and .admx Files | 1. Create a Microsoft 365 trial subscription and test account per Section 3.2.1 if you haven’t already. 2. Download and install the latest windows version of the [new OneDrive sync client](https://go.microsoft.com/fwlink/p/?linkid=844652). 3. Under **All Programs**, select **Microsoft OneDrive** to open app. 4. When OneDrive starts, enter your test account, or your work or school account, created in Section 3.2.1 (USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**) and then select **Sign in**. 5. Browse to **%localappdata%\Microsoft\OneDrive\BuildNumber\adm**, to the subfolder for your language as necessary (Where BuildNumber is the number displayed in sync client settings on the About tab.) 6. Copy the **OneDrive.adml** and **OneDrive.admx** files and store it temporarily in **\\DC1\C$**.   The ADM folder in the OneDrive installation directory |
| **Complete these steps on the DC1 virtual machine.** | |
| Paste .adml and .admx Files in Central Store | 1. In File Explorer, go to the **C:\** drive and copy the **OneDrive.adml** and **OneDrive.admx** files. 2. Go to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions** to your domain's Central Store. 3. Paste the **OneDrive.admx** file in your domain's Central Store and the **OneDrive.adml** file in the appropriate language subfolder (such as **en-US**). **Note:** If you get an “Access Denied” alert when pasting the files, right-click the **Policy Definitions** folder, and then click **Properties>Security>Advanced**. Click the **Permissions** tab, click “**Select principal**” and add “**LabAdmin**” with full permissions. 4. Go to **Server Manager>Tools>Active Directory Users and Computers** and then expand **CORP**. An **Organizational Unit** should have already been created from a previous lab called “**Known Folder**”. 5. Under **Known Folder** ensure that **CLIENT7** and **CLIENT2** exist as done in a previous lab. |
| Configure Group Policy Object | 1. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 2. Right-click the Organizational Unit, example “**Known Folder**” and click **Create a GPO in this domain, and Link it here**. Name the GPO as “**Known Folder**” and click **OK**. 3. Right-click the new GPO “**Known Folder**” and click **Edit**. 4. Go to **Computer Configuration\Policies\Administrative Templates\OneDrive** and **Enable** the following Known Folder Move policy:[Silently move Windows known folders to OneDrive](https://docs.microsoft.com/en-us/onedrive/use-group-policy#silently-move-windows-known-folders-to-onedrive) 5. Add the **Tenant ID** to Known Folder Move Policy. To find the Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 6. Select **Yes** for **Show notification to users after folders have been redirected**. 7. Click **Apply | OK.** For info, see [Link Group Policy objects to Active Directory containers](https://go.microsoft.com/fwlink/?linkid=871796) |
| **Complete these steps on the CLIENT7 AND CLIENT2 virtual machines.** | |
| Confirm Automatic File Transfer | 1. Restart/Start **CLIENT7** and **CLIENT2** to initiate Group Policy and file transfer. 2. Open **CLIENT2** and log into the Microsoft OneDrive app using the same test account as **CLIENT7**. (USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**). 3. Confirm on **CLIENT2** that you get a notification and in both **CLIENT7** and **CLIENT2**, you see **Documents**, **Pictures** and **Desktop** OneDrive folders synced between the 2 machines. |
| **Complete these steps on the DC1, CLIENT7 AND CLIENT1 virtual machines.** | |
| Move Sample Files from Z Drive to SharePoint Shared Library using SharePoint Migration Tool | 1. Create some **Office Sample Files** and create a folder called **Sample Files** on **CLIENT7**’s desktop and then copy the folder to **DC1**’s **C Drive**. 2. In **DC1**’s **C Drive**, right-click **Sample Files** folder and click **Properties**. 3. Click the **Sharing** tab. 4. Click **Advanced Sharing**. 5. Select **Share this folder** and click **Permissions**. 6. Select **Allow – Full Control** and click **Apply** and **OK**. 7. Click **Apply** and **OK** again. 8. Click the **Security** tab and click **Advanced**. 9. Click **Change permissions** and then click **Add**. 10. Click **Select a principal**, type **Everyone** and then click **Check Names**. Click **OK**. 11. Select **Full control** and then click **OK**. 12. Click **Apply** and **OK**. 13. Click **Close**. 14. Log in to **CLIENT1** as **CORP\LabAdmin**, open **File Explorer** and then click **This PC**. 15. From the top, click **Computer | Map network drive | Map network drive**. 16. Select **Z:** next to **Drive** and next to **Folder** enter **\\DC1\Sample Files**. 17. Click **Finish**. 18. Now open **Internet Explorer** and browse to <http://spmtreleasescus.blob.core.windows.net/install/default.htm> to download and install the **SharePoint Migration Tool**. 19. Select **I agree to the Terms of Service and Privacy Policy** and click **Install**. 20. Click **Run** on the prompt and wait for the download and installation to finish. 21. In the **SharePoint Migration Tool** window, the **Sign in** window will open. 22. **Sign in** as **LabAdmin@<AzureDomainName>.onmicrosoft.com**. Click **Start your first migration**. 23. On the **Where’s your content** window, select **File Share**. 24. On the **Select a source** window, click **Choose Folder** and browse to **This PC > Sample Files (\\DC1) (Z:)**. Click **OK**. 25. Click **Next**. 26. In the **Select a destination** window, enter **https://<AzureDomain>.sharepoint.com/**, click **Next** and wait for the **Select a document library** to populate. 27. Select **Documents** and click **Next**. 28. On the Review migration window, name your migration and review other details and click **Next**. 29. On the **Choose your settings** window, click **Migrate**. 30. Once the migration is finished, click **Save** on the prompt. Click the link to the **Communication site**, sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com** and you should be able to see the migrated files/data. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Create a Local GPO for Team Library to Sync Automatically and see Results | 1. On **CLIENT1**, Open **Internet Explorer** and browse to **https://<AzureDomain>.sharepoint.com/**. 2. Click **Site contents** and then click **Documents**. You will be able to see the files that have been migrated from the mapped drive. 3. Click **Sync**, click **Allow/Open**, copy and save the **Library ID** and **Sign in** to the OneDrive sync client. 4. Browse to **%localappdata%\Microsoft\OneDrive\BuildNumber\adm**, to the subfolder for your language as necessary (Where BuildNumber is the number displayed in sync client settings on the About tab.) 5. Copy the **OneDrive.adml** to **C:\Windows\PolicyDefinitions\en-US** and **OneDrive.admx** to **C:\Windows\PolicyDefinitions**. 6. Launch **gpedit.msc**. 7. Go to **Computer Configuration\Administrative Templates\OneDrive**. 8. Double-click on **Configure team site libraries to sync automatically**. 9. Select **Enabled** and click **Show…** 10. Under **Value name** enter **Docs** and under **Value** paste the **Library ID** that was saved earlier. Click **OK**. 11. Click **Apply** and **OK**. 12. Go to **Computer Configuration\Administrative Templates\OneDrive** and **Enable** the following Known Folder Move policy:[Silently move Windows known folders to OneDrive](https://docs.microsoft.com/en-us/onedrive/use-group-policy#silently-move-windows-known-folders-to-onedrive) 13. Add the **Tenant ID** to Known Folder Move Policy. To find the Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 14. Select **Yes** for **Show notification to users after folders have been redirected**. 15. Click **Apply** and **OK**. 16. Go to **Computer Configuration\Administrative Templates\OneDrive** and **Enable** the policy **Use OneDrive Files On-Demand**. 17. Click **Apply** and **OK**. 18. Run a **gpupdate /force** on **CLIENT1**. 19. Open **File Explorer** and click **<AzureDomain>**. 20. In the **File Explorer**, you will be able to notice the files in the **Communication site - Documents** Shared Library and you will be able to note from the symbol if files are in cloud. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create OneDrive for Business Profile in ConfigMgr for moving Windows Known Folders to OneDrive for Business | 1. Find your Microsoft 365 Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 2. Ensure that the client has the latest OneDrive sync client. If you have followed the previous steps, clients have the latest version of the OneDrive sync client as it is in Windows 10. 3. In the Configuration Manager Console, browse to **Assets and Compliance | Compliance Settings | OneDrive for Business Profiles**. 4. Click **Create OneDrive for Business Profile** from the ribbon bar. 5. On the General page, enter the **Name** and click **Next**. 6. On the Supported Platforms page, select **Windows 10** and click **Next**. 7. On the Known Folder Move Settings page, **Specify an Office 365 tenant ID** and either select **Prompt users to move Windows known folders to OneDrive** or **Silently move Windows known folders to OneDrive** and you may also select **Show notification to users after folders have been moved** and **Prevent users from redirecting their Windows known folders back to their PC**. Click **Next**. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. 10. To create a Device Collection, right-click **Device Collections** and click **Folder | Create Folder**. Enter **KFM** and click **OK**. 11. Right-click **KFM** and click **Create Device Collection**. 12. Enter the following details and click **Next**:   Name: **KFM**  Limiting collection: **All Desktop and Server Clients**   1. Click **Add Rule | Direct Rule** and click **Next**. 2. Enter **%ClientName%** and click **Next**. 3. Select the client and click **Next**. 4. Click **Next** and then click **Close**. 5. Click **Next** twice and then click **Close**. Ensure that the client is in the **KFM** collection. 6. Now, to deploy the OneDrive for Business Profile, go back to **Assets and Compliance | Compliance Settings | OneDrive for Business Profiles**. 7. Select the profile created earlier and click **Deploy** from the ribbon bar. 8. Click **Browse…** next to **Collection** and select **Device Collections | KFM | KFM**. Click **OK**. 9. Configure the **Alert** and **Schedule** options and click **OK**. Ensure the first deployment happens immediately. 10. In the client, in the **Configuration Manager Properties | Actions** tab. Run the **Machine Policy Retrieval & Evaluation Cycle** and then click **OK**. In the **Configurations** tab, ensure that the **OneDrive for Business Profile** is visible and click **Refresh** and **Evaluate** until it is **Compliant**. |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create OneDrive Known Folder Move Device Configuration Profiles in Intune | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Browse to **Device configuration | Profiles | + Create profile** and select the following and click **Create**:   Platform: **Windows 10 and later**  Profile: **Custom**   1. Under **Basics** tab, enter the Name: **PoC OneDrive NGSC** and click **Next**. 2. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **ADMX Ingestion**  Description: **OneDrive for Business admx content**  OMA-URI: **./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/OneDriveNGSC/Policy/OneDriveAdmx**  Data type: **String**  Value: **Original content of the OneDrive.admx file to be copied from %localappdata%\Microsoft\OneDrive\BuildNumber\adm**   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **SilentAccountConfig**  Description: **Silently configure OneDrive using the primary Windows account**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/SilentAccountConfig**  Data type: **String**  Value: **<enabled/>**   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMOptInNoWizard**  Description: **Silently redirect Windows known folders to OneDrive**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMOptInNoWizard**  Data type: **String**  Value: **<enabled/> <data id="KFMOptInNoWizard\_TextBox" value="Insert Your Azure Tenant ID"/> <data id="KFMOptInNoWizard\_Dropdown" value="0"/>**  **Note 1:** For Azure Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box.  **Note 2:** Value of 0 = Don’t display any notification and Value of 1 = Display notification after KFM setup has completed.   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMOptInWithWizard**  Description: **Prompt users to move Windows known folders to OneDrive**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMOptInWithWizard**  Data type: **String**  Value: **<enabled/> <data id="KFMOptInWithWizard\_TextBox" value="Insert Your Azure Tenant ID"/>**  **Note:** For Azure Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box.   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMBlockOptOut**  Description: **Prevent users from redirecting their Windows known folder to their PC**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMBlockOptOut**  Data type: **String**  Value: **<enabled/>**   1. Under **Configuration Settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **FilesOnDemandEnabled**  Description: **Enable OneDrive Files On-Demand**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/FilesOnDemandEnabled**  Data type: **String**  Value: **<enabled/>**   1. Once done, click **Next** on the **Configuration Settings** tab. 2. Under **Assignments** tab, click **+ Select groups to include | type and select Sales | click Select | Next**. 3. Under **Applicability Rules** tab, click **Next**. 4. Under **Review + create** tab, click **Create**. 5. On the client side, click **Start | Settings**. 6. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 7. Click **Sync** for the Device Configuration Profiles to be deployed. |

**Note:** Before proceeding with the labs ahead, make sure to move the **CLIENT1**, **CLIENT2** and **CLIENT7** machines back to the Computers container if they are not in the Computers container:

1. In **DC1**, launch **Active Directory Users and Computers**.
2. Navigate to **corp.contoso.com > CORP > Known Folder**.
3. Select and right-click **CLIENT2** and **CLIENT7** and then click **Move…**
4. In the Move menu, under **corp** select **Computers** and then click **OK**.

## User State Migration Tool

For large-scale deployments you can automate much of the process using task sequence-based deployment automation tools such as Configuration Manager or the Microsoft Deployment Toolkit (MDT). Both these solutions make use of User State Migration Tool (USMT) as part of their end-to-end deployment process. USMT is part of the Windows Assessment and Deployment Kit (Windows ADK).

USMT captures user accounts, user files, operating system settings, and application settings, and then migrates them to a new Windows installation. It also gives you, the IT Admin, control of exactly what gets migrated and, optionally, can exclude unwanted file types – for example audio and video files, or executables.

During the migration process you will need to have sufficient server storage capacity available to act as your temporary migration store. Here USMT offers two important features. First, it can estimate, per PC, the amount of storage you will need. Second, it allows for migration stores to be encrypted, reducing the risk of data being compromised while being stored on file servers.

Where you are performing a PC refresh and not reformatting the primary Windows partition, you also have the option of using a hard-link migration store with USMT. This process preserves user state on the PC while the old operating system and apps are removed and refreshed. With the restore process coming from the same local partition, this option offers significant improvements on performance, and reduces network traffic.

In Computer **Refresh**, the key difference is that the user state remains on the disk or will be restored after the install is complete.

In Computer **Replacement**, you replace a PC with another PC. In this case, there is often a backup of user files from the first PC to a central location, then a restore of those files to the second PC.

**Note:** If **CM1** is going to be used for deployments, then **MDT1** should be stopped. Same way, If **MDT1** is going to be used for deployments, then **CM1** should be stopped.

**Prerequisites:**

1. Complete **Section 9.1 - OS Image Creation**.
2. Complete **Section 9.2.1 - Bare Metal**.

### USMT - PC Refresh

In this section, we will refresh a Windows 7 client with Windows 10, keeping all data intact.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the WIN7 and CLIENT1 virtual machines.** | |
| Copy User Data for Migration during a Refresh | 1. Log in to **CLIENT1** and **WIN7** as **CORP\LabAdmin**. 2. Copy the contents of the **CLIENT1** - **Desktop**, **Documents** and **Pictures** from **C:\Users\LabAdmin** to the same locations in **WIN7**. 3. Create another virtual machine checkpoint on **WIN7**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Refresh Device Collection | 1. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **Refresh**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule | Direct Rule** and click **Next** on the Welcome page. 2. In the Search for Resources page, in the Value, enter **WIN7** and then click **Next**. 3. In the Select Resources page, select **WIN7** and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. 6. Back on the Membership Rules page, click **Next**. 7. On the Summary page, click **Next**. 8. On the Completion page, click **Close**. 9. Ensure that the **WIN7** machine is present in the **Refresh** collection. |
| Create a Refresh Task Sequence Deployment | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Deploy Windows 10 X64** Task Sequence and click **Deploy**. 3. On the General page, click **Browse...** 4. Click **OK** on the prompt. 5. Select **Refresh** and then click **OK**. 6. Back on the General page, click **Next**. 7. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Only Configuration Manager Clients** is selected next to Make available to the following. Click **Next**. 8. On the Scheduling page, click **Next**. 9. On the User Experience page, click **Next**. 10. On the Alerts page, click **Next**. 11. On the Distribution Points page, click **Next**. 12. On the Summary page, click **Next**. 13. On the Completion page, click **Close**. |
| **Complete these steps on the WIN7 virtual machine.** | |
| Execute the Refresh Task Sequence Deployment | 1. Click **Start | Control Panel**. 2. Click **System and Security | Configuration Manager**. 3. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 4. Click **Run Now** and then click **OK**. 5. Click the **notification** or open the **Software Center**. 6. Under Operating Systems select **Deploy Windows 10 X64** and then click **Install**. 7. Click **Install** again on the prompt. 8. Notice that the **WIN7** machine installed with Windows 7 will be refreshed with Windows 10 and all user data will be backed up and restored using the User State Migration Tool as part of **PC Refresh**. |

### USMT - PC Replacement

In this section, we will replace a Windows 7 client with a new Windows 10 client, keeping all data intact.

**Prerequisites:**

1. Complete **Section 9.1 - OS Image Creation**.
2. Complete **Section 9.2.1 - Bare Metal**.
3. Complete **Section 7.2.1 or 9.2.2 – PC Refresh**.

**Note:** On **WIN7**, revert to the latest checkpoint.

**Some Workarounds:**

1. When you try to deploy the **Replace Task Sequence** on the Source Computer (**WIN7**) once again or the second time, it might fail accessing the State Migration Point share. The workaround is:
2. Remove the **State Migration Point Role** and delete any folder(s) inside **C:\MigData**.
3. On **WIN7**, in the registry, delete any key(s) under **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SystemCertificates\SMS\Certificates** and reboot **WIN7**.
4. When you deploy the **Windows 10 X64 Task Sequence** on the Destination Computer (**CLIENT6**), it might fail to restore the local computer user profile. The workaround is:
5. Edit the **Windows 10 X64 Task Sequence** and under the **State Restore** Group, select **Restore User State** step.
6. Select **Restore local computer user profiles** and enter the **password** of the **local user account** of the Source Computer (**WIN7**) twice.

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the CM1 virtual machine.** | | |
| Install the State Migration Point | 1. In the Configuration Manager Console, browse to **Administration | Site Configuration | Servers and Site System Roles**. 2. Right-click **CM1.corp.contoso.com** and then click **Add Site System Roles**. 3. On the General page, click **Next**. 4. On the Proxy page, click **Next**. 5. On the System Role Selection page, select **State migration point** and click **Next**. 6. Manually create a folder in **C:\** drive called **MigData** and then on the State migration point page, click the **star** symbol. 7. For the Storage folder, enter **C:\MigData** and click **OK**. 8. On the State migration point page, click **Next**. 9. On the Boundary Groups page, click **Next**. 10. On the Summary page, click **Next**. 11. On the Completion page, click **Close**. | |
| Create a Replace Task Sequence | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Click **Create MDT Task Sequence** from the ribbon bar. 3. On the Choose Template page, select **Client Replace Task Sequence** and click **Next**. 4. On the General page, for the Task sequence name, enter **Replace Task Sequence** and then click **Next**. 5. On the Boot Image page, select **Specify an existing boot image package** and then click **Browse...** 6. Select **MDT Boot Image (x64) en-US** and then click **OK**. 7. Click **Next** on the Boot Image page. 8. On the MDT Package page, select **Specify an existing Microsoft Deployment Toolkit Files package** and then click **Browse...** 9. Select **MDT Files** and then click **OK**. 10. Click **Next** on the MDT Package page. 11. On the USMT Package page, select **Specify an existing USMT package** and then click **Browse...** 12. Select **Microsoft Corporation User State Migration Tool for Windows 10.0.19041.1** and then click **OK**. 13. Click **Next** on the USMT Package page. 14. On the Settings Package page, select **Specify an existing settings package** and then click **Browse...** 15. Select **Windows 10 X64 Settings** and then click **OK**. 16. Click **Next** on the Settings Package page. 17. On the Summary page, click **Next**. 18. On the Confirmation page, click **Finish**. | |
| Create a Replace Device Collection | 1. Browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **Replace**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule | Direct Rule** and click **Next** on the Welcome page. 2. In the Search for Resources page, in the Value, enter **WIN7** and then click **Next**. 3. In the Select Resources page, select **WIN7** and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Completion page, click **Close**. 6. Back on the Membership Rules page, click **Next**. 7. On the Summary page, click **Next**. 8. On the Completion page, click **Close**. 9. Ensure that the **WIN7** machine is present in the **Replace** collection. | |
| Create a New Computer Device Collection | 1. Browse to **Assets and Compliance | Overview | Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. On the General page, enter the following and click **Next**.   Name: **New Computer**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Next**. Click **OK** on the prompt. 2. On the Summary page, click **Next**. 3. On the Completion page, click **Close**. | |
| Associate CLIENT6 with WIN7 | 1. On the Hyper-V Host, start **CLIENT6** for a moment to get the MAC Address of the VM from the **Networking** tab at the bottom and make a note of it. Once noted, turn off **CLIENT6**. 2. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | Devices**. 3. Right-click **Devices** and then click **Import Computer Information**. 4. On the Select Source page, select **Import single computer** and then click **Next**. 5. On the Single Computer page, enter the following and then click **Next**:   Computer name: **CLIENT6**  MAC address: Enter the **MAC Address** which you noted in **Step 48**  Source computer: Click **Search...**, next to Collection click **Browse...**, select **All Systems**, click **OK**, enter **WIN7** next to Computer contains, click **Search**, select **WIN7** from the search results and then click **OK**.   1. On the User Accounts page, under Migration behavior, select **Capture and restore all user accounts** and then click **Next**. 2. On the Data Preview page, click **Next**. 3. On the Collections page, click **Add**, select **New Computer**, click **OK**, select **New Computer** again and then click **Next**. 4. On the Summary page, click **Next**. 5. On the Confirmation page, click **Close**. 6. Click **User State Migration** and review the computer association in the right pane. 7. Select **WIN7/CLIENT6** association and click **View Recovery Information** from the ribbon bar. Note that a user state recovery key has been assigned already, but a user state store location has not. Click **Close**. 8. Ensure that the All Systems collection has the **CLIENT6** VM in it. | |
| Create a Replace Task Sequence Deployment | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Replace Task Sequence** and click **Deploy**. 3. On the General page, click **Browse...** 4. Click **OK** on the prompt. 5. Select **Replace** and then click **OK**. 6. Back on the General page, click **Next**. 7. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Only Configuration Manager Clients** is selected next to Make available to the following. Click **Next**. 8. On the Scheduling page, click **Next**. 9. On the User Experience page, click **Next**. 10. On the Alerts page, click **Next**. 11. On the Distribution Points page, click **Next**. 12. On the Summary page, click **Next**. 13. On the Completion page, click **Close**. | |
| **Complete these steps on the WIN7 virtual machine.** | | |
| Execute the Replace Task Sequence Deployment | | 1. Click **Start | Control Panel**. 2. Click **System and Security | Configuration Manager**. 3. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 4. Click **Run Now** and then click **OK**. 5. Click the **notification** or open the **Software Center**. 6. Under Operating Systems select **Replace Task Sequence** and then click **Install**. 7. Click **Install** again on the prompt and wait for the task sequence to complete after reboot and re-log in. |
| **Complete these steps on the CM1 virtual machine.** | | |
| Verify the Backup | | 1. Browse to **C:\MigData** and verify that a folder was created containing the USMT backup. 2. In the Configuration Manager Console, browse to **Assets and Compliance | Overview | User State Migration**. 3. Select **WIN7/CLIENT6** association and click **View Recovery Information** from the ribbon bar. Note now that a user state store location has been set as well. Click **Close**. |
| Deploy the New Computer CLIENT6 | | 1. Browse to **Software Library | Overview | Operating Systems | Task Sequences**. 2. Right-click **Deploy Windows 10 X64** Task Sequence and click **Edit**. 3. Under the **State Restore** Group, select **Restore User State** step. 4. Select **Restore local computer user profiles** and enter the **password** of the **local user account** of the Source Computer (**WIN7**) twice. Click **Apply** and **OK**. 5. Right-click **Deploy Windows 10 X64** Task Sequence and click **Deploy**. 6. On the General page, click **Browse...** 7. Click **OK** on the prompt. 8. Select **New Computer** and then click **OK**. 9. Back on the General page, click **Next**. 10. On the Deployment Settings page, ensure **Available** is selected next to Purpose and **Configuration Manager clients, media and PXE** is selected next to Make available to the following. Click **Next**. 11. On the Scheduling page, click **Next**. 12. On the User Experience page, click **Next**. 13. On the Alerts page, click **Next**. 14. On the Distribution Points page, click **Next**. 15. On the Summary page, click **Next**. 16. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT6 virtual machine.** | | |
| Execute the New Computer Task Sequence Deployment | | 1. Power on the **CLIENT6** virtual machine and when prompted, press **F12** for network service boot to boot from the boot image available from the PXE distribution point. 2. On the Welcome to the Task Sequence Wizard page, click **Next**. 3. On the Select a task sequence to run page, ensure that **Deploy Windows 10 X64** is selected and click **Next**. 4. When the process is complete, you will have a new Windows 10 machine in your domain with user data and settings restored from **WIN7**. |

## Enterprise State Roaming

With Windows 10, Azure Active Directory (Azure AD) users gain the ability to securely synchronize their user settings and application settings data to the cloud. Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device. Enterprise State Roaming operates similar to the standard consumer settings sync that was first introduced in Windows 8. Additionally, Enterprise State Roaming offers:

* Separation of corporate and consumer data – Organizations are in control of their data, and there is no mixing of corporate data in a consumer cloud account or consumer data in an enterprise cloud account.
* Enhanced security – Data is automatically encrypted before leaving the user’s Windows 10 device by using Azure Rights Management (Azure RMS), and data stays encrypted at rest in the cloud. All content stays encrypted at rest in the cloud, except for the namespaces, like settings names and Windows app names.
* Better management and monitoring – Provides control and visibility over who syncs settings in your organization and on which devices through the Azure AD portal integration.

### Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Prerequisite Lab** | Ensure that both **CLIENT3** and **CLIENT4** virtual machines are freshly (to avoid any conflicts from the previous labs) Azure AD Domain Joined using **TU1@<AzureDomainName>.onmicrosoft.com** and both have been rebooted atleast once. |

### Configure Enterprise State Roaming

In this lab, you will setup and configure enterprise state roaming.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Enable Enterprise State Roaming in the Azure Web Portal | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Devices > Enterprise State Roaming**. 4. In the **Users may sync settings and app data across devices** setting, select **Selected**. 5. Click **Selected** below and click **+ Add**. 6. Type **TU1**, select **Test User1** and click **Select**. 7. Click **OK**. 8. Click **Save**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Confirm that Setting Sync is Enabled for the User | 1. Log in as **TU1@<AzureDomainName>.onmicrosoft.com**. 2. Click on **Start > Settings > Accounts > Sync your settings**. 3. Verify that **Sync your settings** is on. If not on, then turn on **Sync settings**. 4. Verify that the test account is listed in the description of the settings page “Sync your settings to other devices using **<testaccount>**”. |
| Personalize Windows Settings on the First Machine | 1. Right-click on the **taskbar** and uncheck **Lock the taskbar**. 2. Drag the **taskbar** so that it is positioned to the right of the screen. |
| **Complete these steps on the CLIENT3 and CLIENT4 virtual machines.** | |
| Verify that the Changes have Synced to the Second Machine | **Note**: It may take a few minutes for the sync on one machine to propagate to the other. If the sync does not complete. Try logging in and out of both devices or locking and unlocking both the devices or even rebooting both the devices.   1. Log in as **TU1@<AzureDomainName>.onmicrosoft.com**. 2. Verify that the position of the **taskbar** matches the position that was set on **CLIENT3**. |

## Start Menu Customization and UWP App Removal

In this section, you will change the Start Layout of **CLIENT1** for **TestUser1**, use PowerShell to export the Start Layout and then deploy the Start Layout using a Group Policy. You will then be able to see the updated Start Layout in **CLIENT2** for **TestUser1**.

We will also see how to remove a UWP Application.

For more information on Managing Windows 10 Start Layout and the other methods like MDM, Provisioning Packages and PowerShell, refer to <https://docs.microsoft.com/en-us/windows/configuration/windows-10-start-layout-options-and-policies>.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Create a Shared Folder | 1. Open the **File Explorer** and create a new folder by the name **StartLayout** in the **C:\** drive. 2. Right-click **StartLayout** and click **Properties**. 3. Click the **Sharing** tab and then click **Advanced Sharing**. 4. Select **Share this folder** and then click **Permissions**. 5. Select **Allow | Full Control** for **Everyone** and click **Apply | OK**. 6. Click **Apply | OK** again. 7. Click the **Security** tab and then click **Advanced**. 8. Click **Add**. 9. Click **Select a principal**. 10. Type **Everyone** and then click **Check Names**. 11. Click **OK**. 12. Select **Full control** and then click **OK**. 13. Click **Apply | OK**. 14. Click **Close**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Export Start Layout | 1. Log in to **CLIENT1** as **CORP\TestUser1**. 2. Click **Start** and make some Start Layout changes. 3. In the search box, search for **Windows PowerShell** and then click **Windows PowerShell**. 4. Create a folder called **C:\Packages** if not already created and then execute the command - **Export-StartLayout –Path C:\Packages\StartLayoutMarketing.xml** 5. Open the **File Explorer** and navigate to **C:\Packages**. 6. Review the **StartLayoutMarketing.xml** by opening in notepad. Close the file once reviewed. |
| **Complete these steps on the DC1 virtual machine.** | |
| Deploy the Start Layout GPO | 1. Right-click **Start** and then click **Run**. 2. Enter **\\CLIENT1\C$\Packages** and click **OK**. 3. Copy **StartLayoutMarketing.xml** from **CLIENT1** and then paste it to **C:\StartLayout** in **DC1**. 4. Click **Start | Windows Administrative Tools | Group Policy Management**. 5. Expand **Forest:corp.contoso.com | Domains | corp.contoso.com**. 6. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here...** 7. Enter the **Name: Start Layout** and click **OK**. 8. Right-click **Start Layout** and click **Edit...** 9. Navigate to **User Configuration | Policies | Administrative Templates | Start Menu and Taskbar**. 10. Double-click **Start Layout**. 11. Select **Enabled** and under **Start Layout File** enter **\\DC1\StartLayout\StartLayoutMarketing.xml** and then click **Apply | OK**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Check the Start Layout GPO Applied | 1. Log in to **CLIENT2** as **CORP\TestUser1**. 2. Click **Start** and notice that the Start Layout of **CLIENT2** matches with the Start Layout of **CLIENT1**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Remove a UWP Application | 1. Log in to **CLIENT1** as **CORP\LabAdmin**. 2. In the search box, search for **Windows PowerShell** and then click **Windows PowerShell**. 3. Execute the command - **Get-AppxPackage**. This will list all the UWP applications installed. 4. Select one of the UWP application of your choice (example: Crush or Solitaire) that you want to remove by executing the following command - **Get-AppxPackage -Name <Name of the UWP application as per Get-AppxPackage Results>** 5. Copy the **PackageFullName** of the UWP application that you want to remove. 6. Execute the command - **Remove-AppxPackage -Package <PackageFullName as copied before>** 7. Execute the command again to ensure that the UWP application has been removed - **Get-AppxPackage -Name <Name of the UWP application removed>**. There will be no information displayed for the UWP application removed. |

## User Experience Virtualization (UE-V)

Many users customize their settings for Windows and for specific applications. Customizable Windows settings include Microsoft Store appearance, language, background picture, font size, and accent colors. Customizable application settings include language, appearance, behavior, and user interface options.

With User Experience Virtualization (UE-V), you can capture user-customized Windows and application settings and store them on a centrally managed network file share. When users log on, their personalized settings are applied to their work session, regardless of which device or virtual desktop infrastructure (VDI) sessions they log on to. For more guidance, see [**(UE-V) for Windows 10 overview.**](https://docs.microsoft.com/en-us/windows/configuration/ue-v/uev-for-windows)

## Application Self-Service with Microsoft Store for Business

This section will provide the guidance to setup and experience the Microsoft Store for Business. Applications that can be discovered, published and managed using the information contained at the links below.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.**  **Also, log in to https://portal.azure.com and** [**https://www.microsoft.com/en-us/business-store**](https://www.microsoft.com/en-us/business-store) | |
| Access the Microsoft Store for Business | 1. Start a new Internet Explorer window in private mode and access [**https://www.microsoft.com/en-us/business-store**](https://www.microsoft.com/en-us/business-store) 2. Click **Sign in** on the top right-hand corner and sign in using **LabAdmin@<azuredomain>.onmicrosoft.com**, which is a global administrator, created previously and click **Next**. 3. Enter the **password** and click **Sign in**. |
| Roles and Permissions | 1. Click **Manage**. 2. Click **Permissions**. 3. Notice that **LabAdmin** is already assigned the **Global Admin** Role. Click **Assign roles**. 4. In the **Assign roles to people** window, review the various roles available along with their permissions. In the text box above, type **TU1** and click **Test User1** in the search results. You can add multiple users in the text box. 5. Once **Test User1** is added in the text box above, select the Role – **Purchaser** and click **Save**. 6. The user will then be added with the assigned permissions. At any point you want to remove the user from the list, select the user and click **Remove**. For now, do not remove.   **Note**: For more information, refer to <https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business> |
| Find and Acquire Applications | 1. Click **Settings**. Under **Shopping experience**, enable **Show offline apps: Show offline licensed apps to people shopping in the Microsoft Store**. 2. Click **Shop for my group** and click an app of your choice, example **OneNote**. 3. Review the 2 licensing type: **Online** and **Offline**. Select **Offline** and click **Get the app**. 4. If this is the first time you are using Microsoft Store for Business, **check** the **checkbox** for service agreement and click **Accept**. 5. It will mention that the app has been purchased and added to your inventory. Click **Close**. **Offline** apps can be distributed by using a provisioning package and include it as part of imaging a device using Deployment Image Servicing and Management (DISM) or Windows ICD and also can be distributed through a management tool or server.   **Note:** You will then be on the page where it will ask you to manage or download the package for offline use. You do not have to download the package for offline use for this demo. Just go to the **next step**.   1. Under **Shop for my group**, select another app, example **Microsoft Remote Desktop** and select **Online**. Click **Get the app**. 2. It will mention that the app has been purchased and added to your inventory. Click **Close**. It will then present with 2 methods of distribution: By adding to the private store by clicking on the **(… | Manage)** and then **Assign to Users** and **Private store availability**. Online apps can be distributed by assigning it to employees as well as adding it to your private store, allowing employees to download it through a management tool. 3. If you select to add to the private store and decide to assign it to everyone, it will start adding the app into your private store and could take up to twenty four hours before the app is available in the private store as a separate tab. 4. Under **Shop for my group**, select another app, example **Fresh Paint** and click **Get the app**. Click **Close**. If you select **Assign to Users** and then in the text box, type a username, example **TU1**, click **Test User1** in the search results and click **Assign | Close**, the app will be directly available to the user in the Store > My Library section. You can add multiple users in the text box. The user then can download and install the app from the store.   **Note**: For more information, refer to <https://docs.microsoft.com/en-us/microsoft-store/find-and-acquire-apps-overview> |
| App Inventory Management | 1. Click **Manage** and click **Products & services** and click **Apps & software**. 2. You can find an app from the **Search apps & software** text box. 3. You can also refine your search by selecting **Refine results** based on **Product type**, **Application type**, **Source** and **Private store**. 4. You will be able to see the list of apps with the following tabs by clicking **Table view** – **Name, Available quantity, Usage/Total** and **Date**. 5. If you click the **(…)** for an **Online**-licensed app, you will see the options – **View license details**, **Assign to people, View private store details** and **View product details**. 6. If you click the **(…)** for an **Offline**-licensed app, you will see the options – **Download for offline use** and **View product details**. 7. You can even manage app licenses by **viewing**, **assigning** and **reclaiming licenses**.   **Note**: You can remove an app from the Private Store. For more information, refer to <https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business> |
| Distribute Apps with a Management Tool | 1. Click **Manage**, then click **Settings** and then click **Distribute**. 2. You should be able to see the available MDM tools. 3. Select the MDM tool you want to synchronize with Store for Business, and then click **Activate**. Your MDM tool is ready to use with the Store for Business. Consult docs for your management tool to learn how to distribute apps from your synchronized inventory.   **Note**: For more information, refer to <https://docs.microsoft.com/en-us/microsoft-store/configure-mdm-provider-microsoft-store-for-business> |

# Appendix D: Prepare infrastructure

## Outlook Mailbox Hosted Cache Reduction via Group Policy

Cached Exchange Mode gives users a seamless online and offline Outlook experience by caching the user's mailbox and the Offline Address Book (OAB) locally. With Cached Exchange Mode, which is the default setting for users, Outlook no longer depends on continuous network connectivity for access to user information. When a user is connected, Outlook continuously updates users' mailboxes so that the mailboxes are kept up to date. If a user disconnects from the network, for example, by moving to an area without Wi-Fi access, the user can continue to access the last available email data.

In this section, we will configure and deploy the Group Policy for Cached Exchange Mode.

For more information on Additional Group Policy and OCT Settings, refer to <https://docs.microsoft.com/en-us/exchange/outlook/cached-exchange-mode#additional-group-policy-and-oct-settings>

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Check the Default Cached Exchange Mode Setting | 1. Log in as **CORP/LabAdmin** with password **P@ssw0rd**. 2. Log in to <https://login.microsoftonline.com> using **TU1@<AzureDomainName>.onmicrosoft.com** and **Install Office**. 3. Click **Start** and search for **Outlook**. Click **Outlook** from the search results. 4. Enter the username **TU1@<AzureDomainName>.onmicrosoft.com** and click **Connect**. 5. Enter the **password** for **TU1** and click **Sign in**. 6. Uncheck the option **Allow my organization to manage my device** and click **This app only**. 7. Uncheck the box next to **Set up Outlook Mobile on my phone, too** and click **Done**. 8. After Outlook loads, click **Sign in**, sign in as **TU1@<AzureDomainName>.onmicrosoft.com** and click **Accept**. Click **Close**. 9. Click **File | Account Settings | Account Settings...** 10. Select **TU1@<AzureDomainName>.onmicrosoft.com** and click **Change...** 11. Notice that by default, the **Use Cached Exchange Mode to download email to an Outlook data file** is **enabled** and can be enabled/disabled by the user. 12. Cancel all the windows and close Outlook. |
| **Complete these steps on the DC1 virtual machine.** | |
| Download the Administrative Template Files (ADMX/ADML) and Office Customization Tool for Microsoft 365 Apps for enterprise, Office 2019, and Office 2016 | 1. Launch **Internet Explorer** and download the Administrative Template files (ADMX/ADML) and Office Customization Tool for Microsoft 365 Apps for Enterprise, Office 2019, and Office 2016 from [**https://www.microsoft.com/en-us/download/details.aspx?id=49030**](https://www.microsoft.com/en-us/download/details.aspx?id=49030). Click **Download**. 2. Select **admintemplates\_x64\_xxxx-1000\_en-us.exe** and click **Next**. 3. Save the executable file to desktop. 4. Create a folder in the **C:\** drive by the name **Office Admin Templates**. 5. Now from the desktop where you saved the executable file, right-click on the file and click **Run as administrator**. 6. Click **Yes** on the UAC prompt. 7. Select **Click here to accept the Microsoft Software License Terms** and click **Continue**. 8. Browse to **C:\Office Admin Templates** and click **OK**. 9. Once the extraction is completed, click **OK**. 10. Navigate to **C:\Office Admin Templates\admx\** and copy all the folders and files. 11. Then navigate to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions** and paste all the copied files and folders. 12. Select **Do this for all current items** and click **Continue**. |
| Configure the Group Policy for Cached Exchange Mode | 1. Launch the **Group Policy Management** console from the **Windows Administrative Tools**. 2. Expand **Forest:corp.contoso.com | Domains | corp.contoso.com**. 3. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here...** 4. Under **Name** enter **Cached Exchange Mode** and click **OK**. 5. Right-click **Cached Exchange Mode** and click **Edit**. 6. Navigate to **User Configuration > Policies > Administrative Templates > Microsoft Outlook 2016 > Account Settings > Exchange > Cached Exchange Mode**. 7. Double-click **Use Cached Exchange Mode for new and existing Outlook profiles**. 8. Select **Enabled** and click **Apply | OK**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Check the Cached Exchange Mode Setting after the GPO is Applied | 1. Launch an **administrative command prompt** and run a **gpupdate /force**. 2. Click **Start** and search for **Outlook**. Click **Outlook** from the search results. 3. After Outlook loads, click **File | Account Settings | Account Settings...** 4. Select **TU1@<AzureDomainName>.onmicrosoft.com** and click **Change...** 5. Notice that the option, **Use Cached Exchange Mode to download email to an Outlook data file** is **enabled** and now cannot be disabled by the user since this is being applied from the Group Policy. 6. Cancel all the windows and close Outlook. |

## CMPivot for real-time data in Configuration Manager

Configuration Manager has always provided a large centralized store of device data, which customers use for reporting purposes. The site typically collects this data on a weekly basis. CMPivot is a new in-console utility that now provides access to real-time state of devices in your environment. It immediately runs a query on all currently connected devices in the target collection and returns the results. Then filter and group this data in the tool. By providing real-time data from online clients, you can more quickly answer business questions, troubleshoot issues, and respond to security incidents.

**Note:** Before performing the below steps, ensure that the required client machines (atleast **CLIENT1** and **CLIENT2**) in the lab are installed with the latest Configuration Manager client and are turned **ON** and are showing **Active** in **Assets and Compliance > Devices**.

For more information, refer to <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/manage/cmpivot>

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Run CMPivot | 1. In the Configuration Manager Console, navigate to **Assets and Compliance > Device Collections**. 2. Right-click **All Systems** device collection and click **Start CMPivot**. 3. In the **CMPivot (All Systems)** window, click the **Query** tab. 4. Type **OS | summarize dcount( Device ) by Caption** in the query pane and click **Run Query**. 5. Observe the results in the results pane. |

## Outlook Mobile App Config and App Protection

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With **MAM without enrollment** (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any [device](https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform), including personal devices in **bring-your-own-device** (BYOD) scenarios. Many productivity apps, including Microsoft 365 Apps for enterprise, can be managed by Intune MAM. See the official list of [Microsoft Intune protected apps](https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps) available for public use.

For more information, refer to - <https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>

**Note:** You must have an iOS/iPadOS or Android with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create an iOS/iPadOS or Android App Protection Policy | 1. Sign in to [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. In Intune portal, choose **Apps > App protection policies**. This selection opens the **App protection policies** details, where you create new policies and edit existing policies. 3. Select **+ Create policy** and select either **iOS/iPadOS** or **Android**. The **Create policy** pane is displayed. 4. On the **Basics** page, add the following values:  * Name: The name of this app protection policy * Description: [Optional] The description of this app protection policy   The **Platform** value is set based on your above choice.   1. Click **Next** to display the **Apps** page. The **Apps** page allows you to choose how you want to apply this policy to apps on different devices. You must add atleast one app.  * Target to apps on all devices types: Use this option to target your policy to apps on devices of any management state. Choose **No** to target apps on specific device types. For information, see [Target app protection policies based on device management state](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#target-app-protection-policies-based-on-device-management-state) * Device types: Use this option to specify whether this policy applies to MDM managed devices or unmanaged devices. For iOS/iPadOS APP policies, select from **Unmanaged** and **Managed** devices. For Android APP policies, select from **Unmanaged**, **Android device administrator**, and **Android Enterprise**. * Public apps: Click **+ Select public apps** to choose the apps to target. * Custom apps: Click **+ Select custom apps** to select custom apps to target based on a Bundle ID.   The app(s) you have selected will appear in the public and custom apps list.   1. Click **Next** to display the **Data protection** page.   This page provides settings for data loss prevention (DLP) controls, including cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps that this app protection policy applies.  **Data protection settings:**   * **iOS/iPadOS data protection**: For information, see [iOS/iPadOS app protection policy settings – Data protection](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#data-protection). * **Android data protection**: For information, see [Android app protection policy settings – Data protection](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#data-protection).  1. Click **Next** to display the **Access requirements** page.   This page provides settings to allow you to configure the PIN and credential requirements that users must meet to access apps in a work context.  **Access requirements settings:**   * **iOS/iPadOS access requirements**: For information, see [iOS/iPadOS app protection policy settings – Access requirements](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#access-requirements). * **Android access requirements**: For information, see [Android app protection policy settings – Access requirements](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#access-requirements).  1. Click **Next** to display the **Conditional launch** page.   This page provides settings to set the sign-in security requirements for your app protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company apps. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for single setting.  **Conditional launch settings:**   * **iOS/iPadOS conditional launch**: For information, see [iOS/iPadOS app protection policy settings – Conditional launch](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#conditional-launch). * **Android conditional launch**: For information, see [Android app protection policy settings – Conditional launch](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#conditional-launch).  1. Click **Next** to display the **Assignments** page.   The **Assignments** page allows you to assign the app protection policy to groups of users.   1. Click **Next** to review the values and settings you entered for this app protection policy. 2. When you are done, click **Create** to create the app protection policy in Intune.   **Note:** These policy settings are enforced only when using apps in the work context. When end users use the app to do a personal task, they aren't affected by these policies. Note that when you create a new file it is considered a personal file.   1. End users can download the apps from the App store or Google Play. For more information, see:  * [What to expect when your Android app is managed by app protection policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-mam-apps-android) * [What to expect when your iOS/iPadOS app is managed by app protection policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-mam-apps-ios) |